

REQUEST FOR PROPOSAL

For

Selection of Service Provider for
Implementation of
Cyber Security Solutions and CSOC
for VSCDL (Second Attempt)

Tender No.: VSCDL/499/2020-21



Issued by

Vadodara Smart City Development Limited (VSCDL)

Vadodara

Table of Contents

1	Invitation for Proposal.....	9
1.1	RFP Notice.....	9
1.2	Important Dates / Information	9
1.3	Notice of Confidentiality	10
2	Introduction and Background	11
2.1	About Vadodara.....	11
2.2	About Vadodara Smart City Development Limited (VSCDL)	11
2.3	Project Objective.....	11
2.4	About Smart City IT Projects.....	12
2.5	Need for Strengthening IT Security	13
2.6	Security Risk Landscape by Indian Smart Cities	13
2.7	MoHUA and India's Journey into Cybersecurity	15
3	Pre-Qualification Criteria and OEM Selection Criteria.....	17
3.1	Pre-Qualification Criteria	17
3.2	OEM Selection Criteria.....	20
4	Instructions to Bidder.....	21
4.1	Availing Bid Documents	21
4.2	Completeness of the RFP.....	21
4.3	Proposal Preparation Cost.....	22
4.4	Pre-Bid Meeting (Virtual).....	22
4.5	Conflict of Interest.....	23
4.6	Amendment of RFP Document	23
4.7	VSCDL's Rights to Terminate the Selection Process.....	24
4.8	Right to Reject Any Proposal.....	24
4.9	Tender Fee and Earnest Money Deposit (EMD)	25
4.10	Sealing, Marking and Submissions of Bids	26
4.11	Language of Bids.....	28
4.12	Concessions Permissible under Statutes	28
4.13	Bid Validity	28
4.14	Firm Prices and Bid Currency	28
4.15	Right to Vary the Scope of the Work at the Time of Award.....	28
4.16	Modification or Withdrawal of Bids	28
4.17	Bid Submission Format	29
4.18	Documents Comprising of Bids	29
4.19	Evaluation Process.....	30

4.20	Technical-Qualification Criteria and Evaluation of Technical Bids	30
4.21	Technical Presentation and Demonstration	32
4.22	Opening and Evaluation of Commercial Bid	33
4.23	Award Criteria.....	33
4.24	Rights to Accept/Reject any or all Proposals	34
4.25	Notifications of Awards and Signing of Contract	34
4.26	Quantity Variation	34
4.27	Performance Bank Guarantee	34
4.28	Vandalism/Force Majeure.....	35
4.29	Failure to Agree with the Terms & Conditions of the RFP/Contract	35
4.30	Terms and Conditions of the Tender	35
5	Scope of Work.....	36
5.1	Detailed Scope of Services	36
5.2	Project Planning & Management	53
5.3	Systems Audit.....	53
5.4	Review for IT Infrastructure	55
5.4.1	IT Process Review	55
5.4.2	Change Management Review.....	55
5.4.3	Incident Management Review	55
5.4.4	Asset Management Review	55
5.4.5	Anti-virus and Patch management process Review.....	56
5.4.6	Third Party management Review	56
5.4.7	User access management Review	56
5.4.8	Backup management Review	56
5.4.9	Training and awareness programs Review	56
5.4.10	Desktop Review.....	57
5.4.11	Physical and Environmental Security management Review	57
5.4.12	IT Infrastructure Configuration Review	57
5.4.13	Operating Systems Review.....	57
5.4.14	Database Review	58
5.4.15	Review of Network Devices.....	58
5.4.16	Vulnerability Assessment and Penetration Testing.....	59
5.4.17	Network Performance Review	59
5.4.18	Network Architecture Review	60
5.5	Professional Project Management.....	60
5.6	Use & Acquisition of Assets during the term.....	60
5.7	Security and safety.....	61

6	Functional and Technical Requirements.....	62
6.1	Security Information and Event Management (SIEM).....	62
6.2	Cyber Security Solution Components	64
6.2.1	Next Generation Firewall (NGFW)	67
6.2.2	Web Application Firewall (WAF).....	70
6.2.3	VSCDL Requirement for Additional Licenses of Antivirus	73
6.2.4	HIPS	73
6.2.5	Data Loss Protection (DLP)	75
6.2.6	SIEM	78
6.2.7	Anti - Advanced Persistent Threat (Anti-APT).....	84
6.2.8	Network Access Control (NAC).....	86
6.2.9	Integration / Repositioning of Existing HSM.....	87
6.3	VAPT Information and Remediation Services	87
6.4	Security/Threat Intelligence Services	88
6.5	Hardware, Software and Network Connectivity.....	89
6.6	Training	89
6.7	Implementation & Integration	90
6.8	Reporting.....	93
6.9	System Integration Testing (SIT) and User Acceptance Testing (UAT)	94
6.10	Monitoring.....	94
6.11	Continuous Improvement	96
6.12	SLA Compliance.....	96
6.13	Business continuity.....	96
6.14	Period of Contract.....	96
6.15	Deployment of CSOC Operations Personnel during O&M Period	98
7	Project Phases, Work Completion Timelines & Payment Terms	100
7.1	Project phases.....	100
7.2	Request Orders –.....	100
7.3	Further milestones and payment schedules.....	100
8	Service Level Agreement.....	104
8.1	Service Level Agreement	104
8.1.1	SLA for Project Implementation.....	105
8.1.2	SLA for System Uptime (Solution Uptime)	105
8.1.3	SLA for Maintenance and Support Term.....	107
8.2	SLA Exclusions	111
8.3	Issue and Escalation Management Procedures.....	111
8.4	Issue Management Procedures	111

8.5	SLA Change Control	112
8.6	SLA Change Process	112
8.7	Version Control	112
8.8	Responsibilities of the Parties	112
8.8.1	Responsibilities of the Selected Vendor.....	112
8.8.2	Responsibilities of the VSCDL	112
8.9	Management Escalation Procedures and Contact Map	113
9	Annexure I: Instructions for Pre-Qualification Bid.....	114
9.1	Pre-Qualification Cover Letter	114
9.2	Check-list for the documents to be included in the Pre-Qualification Folder	115
9.3	PQ_1: Bank Guarantee for Earnest Money Deposit (EMD)	117
9.4	PQ_2: Bidder Information Format	118
9.5	PQ_3: Power of Attorney	119
9.6	PQ_4: Bidder's Turnover Details and Net Worth	120
9.7	PQ_5: Experience of Implementing Cyber security /CSOC related projects.....	121
9.8	PQ_6: Undertaking for Technically Qualified Full-time Professionals on Company's Payroll 123	
9.9	PQ_7: Self Declaration – No Blacklisting	124
9.10	PQ_8: Self Declaration – Bidder Not Terminated, Not Being Insolvent or In Receivership or Bankrupt.....	125
10	Annexure II: Instructions for Technical Bid.....	126
10.1	General Instructions for Preparation of the Technical Proposal	126
10.2	Documents Checklist for Technical Bid.....	128
10.3	TQ_1: Bidder's Turnover Details and Net Worth.....	130
10.4	TQ_2: Experience of Implementing IT/ICT Projects.....	132
10.5	TQ_3: Undertaking for Technically Qualified Full-time Professionals on Company's Payroll.....	134
10.6	TQ_4: Undertaking for Manpower Deployed on Project	135
10.7	TQ_5: CVs of the Manpower Proposed	136
10.8	TQ_6: Format for Authorization Form (MAF) from OEMs.....	138
11	Annexure III: List of Products/Solutions which require MAF from OEMs.....	139
12	Annexure IV: Commercial Proposal Formats	140
12.1	Commercial Proposal Cover Letter.....	140
12.2	Commercial Bid Formats.....	142
13	Annexure V – List of IT Projects	149
14	Annexure VI- Common guidelines/requirements regarding compliance of equipment	152

RFP for Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL
(Second Attempt)

15	Annexure VII: Format for Performance Bank Guarantee	154
16	Annexure VIII: Master Service Agreement	156
17	Annexure IX: Non-Disclosure Agreement.....	174

General Glossary

Term	Meaning
API	Application Program Interface
BOM	Bill of Material
CCC	Command and Control Centre
CCTV	Closed Circuit Television
CSP	Cloud Service Provider
DC	Data Center
DR	Disaster Recovery
EMD	Earnest Money Deposit
FRS	Functional Requirements Specifications
GoG	Government of Gujarat
GoI	Government of India
GPS	Global Positioning System
HOD	Head of Department
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technology
INR	Indian Rupee
iPole	Intelligent Pole
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
KVM	Keyboard Video Mouse
LED	Light Emitting Diode
LoI	Letter of Intent
MAF	Manufacturer's Authorization Form
MFP	Multi-Functional Printer
NOC	Network Operation Center
NPV	Net Present Value
O&M	Operation & Maintenance
OEM	Original Equipment Manufacture
POP	Point of Presence
QoS	Quality of Service
RFP	Request for Proposal
RV	Revenue (RV1-Revenue from 1, RV2-Revenue from 2)
SLA	Service Level Agreement
SOR	Schedule Of Rates
SPV	Special Purpose Vehicle

SRS	Software Requirement Specifications
TDS	Tax Deducted at Source
TQ	Technical Qualification
VM	Virtual Machine
VMC	Vadodara Municipal Corporation
VPN	Virtual Private Network
VSCDL	Vadodara Smart City Development Limited

Information Security Glossary

Acronym	Description
APT	Advanced Persistent Threat
CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional
CSOC	Cyber Security Operations Center
DC	Data Center
DR	Disaster Recovery
DRS	Disaster Recovery Site
EPS	Events Per Second
ISMS	Information Security Management System
ITV	Information Technology Vertical
LA	Lead Auditor
LI	Lead Implementer
MSSP	Managed Security Services Provider
NAC	Network Access / Admission Control
NDA	Non-Disclosure Agreement
NIPS	Network Intrusion Prevention System
NPV	Net Present Value
PDC	Primary Data Center
PIM	Privilege Identity Management
RCB	Registered Certification Body
RiMV	Risk Management Vertical
SI	System Integrator
SIEM	Security Information & Event Management
SLA	Service Level Agreement
SPEC	Standard Performance Evaluation Corporation
VAPT	Vulnerability Assessment & Penetration Testing
WAF	Web Application Firewall

1 Invitation for Proposal


1.1 RFP Notice

This RFP document is being published by the Vadodara Municipal Corporation, for the Project of “**Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)**”.

Bidder agencies are advised to study this RFP document carefully before submitting their proposals in response to the RFP Notice. Submission of a proposal in response to this notice shall be deemed to have been done after careful study and examination of this document with full understanding of its terms, conditions and implications.

This RFP document is not transferable.

1.2 Important Dates / Information

	Vadodara Smart City Development Limited (VSCDL) C/o Vadodara Municipal Corporation, Khanderao Market, Vadodara Notice Inviting RFP for “ Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt) ”
Bid for Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt) is invited online on (n) Procure website (https://vmc.nprocure.com/) from the bidder meeting the basic eligibility criteria as stated in the bid document.	
RFP Document Availability	(n)Procure website (https://vmc.nprocure.com/)
Tender Fee (Non-refundable)	Tender Fee of INR 10,000/- plus GST (total amount 11,800/-) by Demand Draft only in favour of “ Vadodara Smart City Development Limited ”.
EMD	EMD of INR 20,00,000/- (Rupees Twenty Lakhs only) shall be either in form of <ul style="list-style-type: none">• Demand Draft in favour of “Vadodara Smart City Development Limited” from any nationalized/scheduled banks, payable at Vadodara OR <ul style="list-style-type: none">• Bank Guarantee issued by Nationalized Bank including Private Banks – Axis Bank, HDFC Bank and ICICI Bank along with other banks mentioned in the GR of Finance Department of Government of Gujarat (GR No EMD/10/2019/50/DMO dated 01/11/2019 and its subsequent revisions) only in favour of “CEO, Vadodara Smart City Development Limited”.
Start date and time for downloading RFP	17 th September 2020
Deadline for submission of pre-bid queries for	22 nd September 2020 at 1100 Hrs

clarifications	
Date, time and place of pre-bid meeting	24 th September 2020 at 1530 Hrs Meeting mode : Virtual, On video conferencing platform such as Zoom/Google Meet etc – Meeting ID will be shared via email before pre-bid)
Deadline for submission of Proposal and EMD, online	9 th October2020 at 1600 Hrs
Deadline for physical submission of technical Proposal, Tender Fee and EMD	12 th October2020 at 1700 Hrs Address: <i>Vadodara Municipal Corporation, Smart city Office, Khanderao Market, Vadodara – 390209, Gujarat</i>
Date, time and place of online opening of Technical Proposals	To be informed later. <i>Place: VSCDL, C/o Vadodara Municipal Corporation</i>
Date, time and place of presentation/demo on Technical Solution by bidders	To be informed later. <i>Place: VSCDL, C/o Vadodara Municipal Corporation</i>
Date, time and place of online opening of Financial Proposals	To be informed later. <i>Place: VSCDL, C/o Vadodara Municipal Corporation</i>
Contact for queries	IT Department, Vadodara Smart City Development Limited, C/o Vadodara Municipal Corporation Khanderao Market, Vadodara – 390001, Gujarat Email ID: smartcity_itcell@vmc.gov.in

The right to accept/reject any or all bid(s) received is reserved without assigning any reason thereof.

General Manager (IT)
Vadodara Smart City Development Limited

1.3 Notice of Confidentiality

This document, its appendices, and all annexes, are the property of VSCDL. Use of contents of document, its appendices, and all annexes is, provided to you for the sole purpose of responding to this Request for Proposal. It may not be otherwise copied, distributed or recorded on any medium, electronic or otherwise without VSCDL's express written permissions.

2 Introduction and Background

2.1 About Vadodara

Located in western part of India in the state of Gujarat, Vadodara (formerly known as Baroda) is referred as cultural capital of Gujarat and is the third largest city after Ahmedabad and Surat. It is the administrative headquarters of Vadodara District and is located on the banks of the Vishwamitri River. As per the Census 2011, it has a population of almost 1.7 million+ people. The city is an important industrial, cultural and educational hub of western India and has the largest university in Gujarat, the Maharaja Sayajirao University of Vadodara. The city houses several institutions of national and regional importance while its major industries include petrochemicals, engineering, chemicals, plastics, IT and pharmaceuticals and foreign exchange services amongst others.

2.2 About Vadodara Smart City Development Limited (VSCDL)

Vadodara has also been selected as one of the sixty Indian cities (in the Second round of selection) to be developed as a smart city under Smart Cities Mission.

One of the primary objective of Vadodara under its smart city mission is to enhance the safety and security, improve efficiency of municipal services and promote a better quality of life for residents. In order to achieve these objectives, Vadodara desires to foster the development of a robust ICT infrastructure that supports digital applications and ensures seamless steady state operations, traffic management, surveillance, emergency response mechanisms and real time tracking of services and vital city metrics throughout the city and in government departments.

As per the GoI guidelines, Vadodara Municipal Corporation has formed a separate Special Purpose Vehicle (SPV) as Vadodara Smart City Development Limited (VSCDL) for the implementation of projects under the smart city mission for the city of Vadodara. This SPV has been entrusted with end to end responsibility for bid process/procurement, implementation and operationalization of various smart city projects.

2.3 Project Objective

The following paragraphs replaces the section 2.3 of the RFP and the project objective are as follows:

VSCDL has decided to build a Cyber Security Operation Centre (CSOC) to monitor, assess and defend VSCDL 's information systems in order to protect confidentiality, integrity and availability of the VSCDL data.

The proposed CSOC facility is to be equipped with set of tools such as Security Information and Event Management Tool (SIEM) and other cyber security components given in detail under this RFP and Security Intelligence services for better security monitoring and response capabilities. VSCDL intends to implement Cyber-Security Operation Centre (CSOC) for information assets at Primary Data Center and DR site. VSCDL expect Service provider to provide full-fledged Services including but not limited to design, supply, implementation, configuration, customization, integration, monitor, manage, backup, documentation, training, warranty support, post warranty maintenance support, back to back arrangement with OEM and any other activities related to or connected to the Information Technology / Cyber security solutions, devices & technologies. The bidder should provide cyber security services for the project listed in section 1.15 of the corrigendum.

The bidder is expected to do following but not limited to:

- a) Design, implement, manage and monitor CSOC
- b) Security Monitoring of attacks into/on/against VSCDL's IT assets
- c) Manage security, configuration, availability, performance and fault management, advisory for the security devices and its software stipulated in scope.
- d) Ensure Malware Scanning / Protection/ Presentation /Reporting as required by the VSCDL including total Anti-APT solution.
- e) Provide proactive threat intelligence and threat hunting.
- f) Vulnerability Assessment & Penetration Testing for critical devices/ servers /applications/solutions at (1) initially during the project implementation (2) Yearly basis during the O&M period of this project and provide solution for closure
- g) Risk assessment and mitigation, protection, execution support for the Security solutions, devices, software and tools under the scope of CSOC.
- h) Prepare VSCDL's Information Security Policy and Cyber Security Policy and ensure adherence of the same
- i) Ensure adequacy, appropriateness and concurrency of various policies as per the requirement of regulatory authorities and Government of India Security authorities, IT Act 2000 and subsequent amendments and guidelines in place.
- j) Provide Cyber/IT Security forensics support as per the requirement of VSCDL in case of any incident or as and when required.
- k) Dashboard for reporting and SLA management.
- l) The selected Bidder will be responsible for implementing CSOC at central location identified by VSCDL, i.e. DC site. Selected Bidder will also supply and install all required infrastructure for operations of the CSOC as per the broad objectives outlined in this section & detailed scope of RFP.
- m) As proposed in this bid, the SIEM tool and other security solutions have to be implemented in the VSCDL premises and the procured security solutions to be integrated with SIEM tool. The proposed CSOC service should cover security event correlation, monitoring, incident management and providing proactive security alert and remediation. The selected bidder will be playing responsible for implementation and management of CSOC for all the security solutions/tools as detailed in Section 4.
- n) Contain the cyber security attacks and IT Forensic capability on need basis for specific incidents
- o) The bidder has to perform hardening of devices which are procured as part of this project and suggest hardening of any other device of Vadodara Smart City Projects which are being monitored through CSOC. The respective SI will be responsible such hardening of their own devices.
- p) Support third party information security audit initiated by VSCDL (Once every year) during the contract period
- q) Ensure future integration with new applications and devices as part of CSOC operations during contract period.

2.4 About Smart City IT Projects

Currently VSCDL and VMC are executing the following Projects

- VMC's applications at Kharderrao Market Server Room
- CCC and its subprojects (Smart city Data Centre)
- ITMS (Smart city Data Centre)
- ERP (Smart city Data Centre)

- HMIS (on Cloud)
- Water SCADA and Drainage SCADA (Smart city Data Centre)
- Smart Street Light ((Smart city Data Centre and cloud)
- GIS ((Smart city Data Centre)
- Public Wi-Fi and iPoles (Smart city Data Centre)
- My Vadodara Mobile App (on Third Party site)
- Other upcoming IT Projects

Annexure V provides more details about these projects and systems to be covered as part of Information Security Analysis.

2.5 Need for Strengthening IT Security

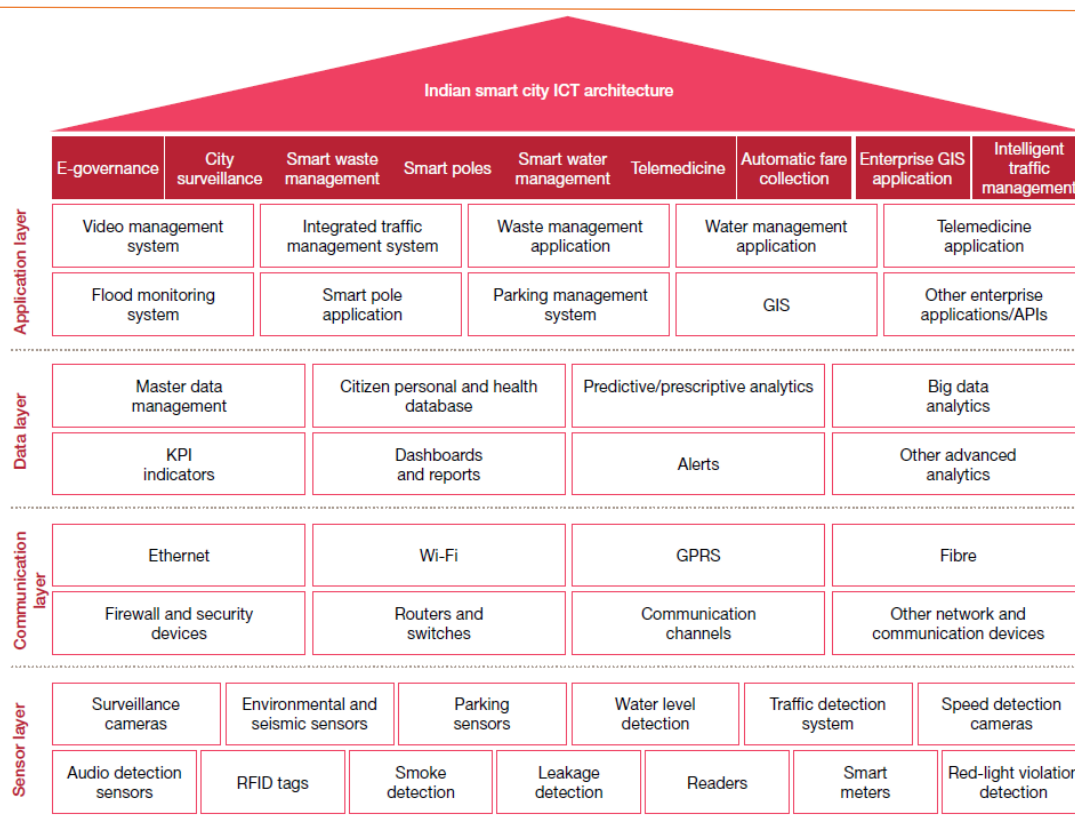
Vadodara Smart City Projects as listed above may be exposed to a diverse set of cyber security threats and criminal misuses compromising the essence of cyber security.

Sr No	Categories	Possible IT Security threats
1	Digital Centric Flagship Projects	Smart Cities are digital centric and composed of electronic devices with ability of internet-active data exchange through wired or wireless means.
2	Smart devices/ Edge devices	Smart devices/Edge devices may be remotely accessible making them more susceptible to hacks
3	Sensitive customer data	Smart city contains sensitive customer data and other financial data making it more susceptible to attract cyber threats
4	Extensive Network with multiple access points	There are VPNs, e-mail, web and network services that are potential target points for attacks through malwares, social engineering/spear phishing, brute force & DDOS attacks, MITM, DNS attacks etc.
5	Massive scale and coverage	The scale or coverage of Smart city initiative is large that can impact two main stakeholders i.e. government and citizens

2.6 Security Risk Landscape by Indian Smart Cities

The Indian Smart City technology architecture can be understood through the four logical layers: sensor, communication, data and application layers. The technology across these four layers works in an integrated manner to deliver Smart City services. The following diagram describes the standard Indian Smart City ICT Architecture, which is more or less followed for Vadodara Smart City also.

RFP for Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)



Our analysis and on-ground assessment of a few smart cities suggest that the technology powering the Indian smart city services are very much prone to vulnerabilities, which can lead to potential social, health, economic and/or reputational risks. The presence of inherent challenges, lack of granular guidelines and regulations, and India-specific issues add to the complexity of the risk landscape for Indian smart cities

Smart Service	Vulnerabilities in systems associated with smart service	Potential risks
E-governance	Unencrypted storage and transmission of citizen data <ul style="list-style-type: none"> • Lack of user access and authorisation controls • Multiple vulnerabilities due to non-adherence to software development life cycle (SDLC) process • Outdated version prone to emerging attacks including Ransomware 	Citizen personal data, including financial and health data, can be compromised <ul style="list-style-type: none"> • E-governance services can be shut down, denying services to citizens
City surveillance	Default password and configuration <ul style="list-style-type: none"> • CCTV cameras accessible over open Internet with weak access controls • Insecure transmission of video feeds 	Video surveillance can give information about weak surveillance zones which can be used for malicious antisocial purposes and to plan and plot a city-level attack <ul style="list-style-type: none"> • Video recordings can be tampered/deleted, hampering police investigation
Smart poles	Default password and configuration of smart pole edge devices (e.g. Wi-Fi, sensors) <ul style="list-style-type: none"> • Inappropriate validation mechanism for connecting to edge devices (e.g. Wi-Fi) 	Attackers may connect to Wi-Fi and send anti-social emails to create unrest in the city <ul style="list-style-type: none"> • Anti-political message can be displayed in public places

	<ul style="list-style-type: none"> • Remote terminal access to sensors 	through digital billboards to stir unrest amongst the public <ul style="list-style-type: none"> • Lights can be put off at night so that a crime is not captured by surveillance cameras
Intelligent traffic management system	Man-in-the-middle attack between sensor and reader <ul style="list-style-type: none"> • Cloning and spoofing • Denial of service attacks 	Miscreants can monitor the live location of buses and other parameters to plan an attack <ul style="list-style-type: none"> • Traffic signals can be manipulated to create a traffic jam in the city
Smart water management	Tampering of data during storage/transmission <ul style="list-style-type: none"> • Cloning and spoofing • Denial of service attacks 	Wrong data related to water management can lead to water shortage, unidentified wastage of potable water, and unavailability of water quality control metrics
Enterprise GIS Application	Unpatched vulnerabilities in GIS applications/application program interfaces (APIs) <ul style="list-style-type: none"> • Insecure cross-system communication 	Unauthorised access can be gained to critical city plans/layout <ul style="list-style-type: none"> • Cross-system communication can be hijacked to further propagate attacks

2.7 MoHUA and India's Journey into Cybersecurity

India's efforts to protect its smart cities are timely. A host of policies and regulations have been designed to protect the smart city infrastructure from cyberattacks. Some of the existing/upcoming regulations on security and privacy are also applicable to smart cities, thereby helping to build secure cities.

Sr No	Organisation	Intitatives
1	Ministry of Housing and Urban Affairs (MoHUA) Guidelines	MoHUA, the Government of India, released a model framework for cyber security in smart cities on 20 May, 2016. It covers the security of smart cities across different layers, namely sensor layer, communication layer, data layer and application layer. The major guidelines include, but are not limited to: <ul style="list-style-type: none"> • Designing a secure network architecture based on the National Institute of Standards & Technology (NIST) reference IT architecture 2• Security solutions that needs to be considered while developing a smart city • Secure storage and transmission of data between different systems and devices implemented in the smart city • Security assessment of the services before and after going live • Compliance with standards such as ISO 27001, ISO 22301, ISO 37120, ISO 3712, ISO 27017, ISO 27018, BSI PAS 180, BSI PAS 182, Protected Extensible Authentication protocol (PEAP) and 3rd generation Partnership Project (3GPP), as applicable • Setting up of security monitoring for smart city network, devices and sensors • Reporting of security incidents to relevant bodies such as Computer Emergency Response Team – India (CERT-In) and

		National Critical Information Infrastructure Protection Centre (NCIIPC).
2	The National Critical Information Infrastructure Protection Centre (NCIIPC), 2014:	NCIIPC has been identified as the nodal agency under the National Technical Research Organisation for the protection of critical information infrastructure. The formal roles and responsibilities of the NCIIPC include cooperation strategies, issuing guidelines, advisories and coordination with CERT-In. The NCIIPC has defined controls for the critical infrastructure sectors to enhance security
3	National Cyber Security Policy, 2013:	The policy aims to create a secure cyber ecosystem in the country and strengthen the regulatory framework
4	Information Technology Act (IT Act), 2000, and its amendments	The IT Act includes rules on the protection of sensitive personal data or information and provisions for electronic service delivery, publication of content of a specific nature on the Internet, and the penalties applicable in case of any offence
5	Aadhaar Act, 2016, and its regulations:	The Aadhaar Act, 2016, defines how Aadhaar-related data is to be captured, stored and processed. Aadhaar data includes not only biometric information (fingerprints, iris and photo) but also the demographic details of the resident. The Aadhaar Act, 2016, forms the basis of various e-governance initiatives such as distribution of services and benefits to residents of India.
6	Draft Personal Data Protection Bill:	The Personal Data Protection Bill includes provisions to protect personal data as an essential facet of information privacy. The bill provides guidelines on the data processing grounds, rights of the data principal, penalties and exemptions, amongst other areas. The bill aims to protect the autonomy of individuals from data privacy violations by the state and private entities. Once enforced, the bill will impact how the smart city information systems store and process personal/sensitive data
7	Draft Digital Information Security in Healthcare Act (DISHA):	The draft DISHA document was recently released in the public domain for comments. It aims to set up a National Health Authority in India which shall be responsible for enforcing privacy and security measures for electronic health data, and to regulate storage and exchange of the same

In line with the evolving Cyber Threat Landscape, GoI has laid guidelines to design Smart City Cyber Security (MoHUA Guidelines vide Circular No. K- 15016/I. There is need to assess the current IT Infrastructure of various IT Projects of Vadodara Smart City

3 Pre-Qualification Criteria and OEM Selection Criteria

3.1 Pre-Qualification Criteria

The pre-qualification criteria for participating in this tender are mentioned in the table below.

#	Pre-Qualification Criteria	Proof Document Required								
1.	The bidder must be a company in India Registered under The Companies Act 1956/The Companies Act 2013 (& subsequent relevant amendments) or a Limited Liability Partnership Firm under Limited Liability Partnership Firm Act 2008 and should be operational at least for last 5 years as on date of Publishing of RFP.	Copy of Certificate of Incorporation.								
2.	The bidder should have a positive net worth and should be a profit-making company, as on 31 March 2019.	Certificate from the statutory auditor/CA clearly specifying the net worth of the firm								
3.	The bidder should have average annual turnover of at least Rs. 30 Cr from Information Technology business in India, for last three audited financial years and must have 15 cr. Annual turnover from Information Security/Cyber Security Business in India for any of last two audited financial years	CA certified and audited Balance Sheet and Profit & Loss statement for last three financial years (2016-17, 2017-18, 2018-19). CA certificate mentioning turnover from the said business.								
4.	<p>The bidder must have at least 50 Professional employees on its payroll in India, with at least 10 employees having a minimum of 3 years of experience in Information Security domain and having certificate in following combination:</p> <p>Minimum 10 certified employees across all categories. (Minimum one professional certified employee from each of the below category)</p> <table><tr><th>Category</th><th>Certification*</th></tr><tr><td>A</td><td>BS7799 or BS17799 or ISO27001 Lead Auditor or ISO27001 Lead Implementers</td></tr><tr><td>B</td><td>CISA/CISM/CISSP</td></tr><tr><td>C</td><td>CEH or GCIH or CHFI or OSCE or ECSA</td></tr></table> <p>*Valid certification from an accredited certifying agency.</p>	Category	Certification*	A	BS7799 or BS17799 or ISO27001 Lead Auditor or ISO27001 Lead Implementers	B	CISA/CISM/CISSP	C	CEH or GCIH or CHFI or OSCE or ECSA	Certificate from HR head confirming compliance.
Category	Certification*									
A	BS7799 or BS17799 or ISO27001 Lead Auditor or ISO27001 Lead Implementers									
B	CISA/CISM/CISSP									
C	CEH or GCIH or CHFI or OSCE or ECSA									

	<i>(Resources with multiple certificates shall be counted once only. And such resources should be self-classified in one of the above categories)</i>	
5.	<p>The bidder should have executed assignments within last three years. for Information Security services business, with each project value as follows</p> <ul style="list-style-type: none"> One project of at least Rs. 7 Crores <p>OR</p> <ul style="list-style-type: none"> Two projects of at least Rs 3.5 crores <p>Information Security services business is defined as implementing and supporting SOC/CSOC, implementing Cyber security hardware/software solutions#, #Hardware/software solution comprises of SIEM + at least one of the following.</p> <ol style="list-style-type: none"> Next Generation Firewall NAC Anti APT PIM Endpoint Detection and Response (EDR) 	<p>Copy of</p> <ol style="list-style-type: none"> Work Order Agreement (*) Work Completion i.e. (Completion of Implementation & Go-Live) Certificate <p>clearly depicting the scope of work, contract period and project value and Client contact details with Mobile number, Landline number and Email ID</p> <p>Note (*) If the said assignment is under NDA then a declaration from the bidder is required depicting the NDA situation but all the information which is needed in order to check the compliance of this criteria must be furnished.)</p>
6.	<p>The bidder should have executed assignments within last three years, for IT Governance*, IT Assessment, IT Governance, risk and compliance (IT GRC) or Information Security Policy Implementation, with each project value as follows:</p> <ul style="list-style-type: none"> One project of at least Rs. 50 Lakh <p>OR</p> <ul style="list-style-type: none"> Two projects of at least Rs 25 lakhs <p>OR</p> <ul style="list-style-type: none"> Five projects of at least Rs. 10 lakhs <p>Out of the above projects, at least one project should have been implemented in Government/PSU/ULB in India assessing Cyber security hardware/cyber security software solutions and providing information security / cyber security services.</p> <p>*IT Governance Definition – Processes that ensures effective and efficient use of IT in enabling the organization to achieve its goal. It's a set of rules, regulations and policy that defines and ensures the effective control & valuable operations of IT assets.</p>	<p>Copy of Work Order of the project from the client clearly depicting the scope of work, contract period and project value.</p> <p>And</p> <p>Copy of Work Completion Certificate from the client</p> <p>And</p> <p>Client contact details with Mobile number, Landline number and Email ID</p>
7.	The Bidder must have a valid ISO 27001 certificate as on date of publishing of the RFP	Copy of valid ISO 27001 certificate
8.	The bidder should have valid GST registration number.	Copy of relevant GST certificate.

9.	The bidder should have submitted valid Income Tax Returns for the last three financial years (i.e. 2016-17, 2017-18 and 2018-19) and the bidder (not individual) should have valid PAN Card.	Copy of Income Tax Returns (ITR) and ITR acknowledgment form for the last three financial years and copy of PAN card.
10	As on date of submission of the proposal, the bidder should not be blacklisted by Central/State Governments in India.	Undertaking by the authorized signatory as per format
11	<p>The bidder should:</p> <ul style="list-style-type: none"> not be insolvent, in receivership, bankrupt or being wound up, not have its affairs administered by a court or a judicial officer, not be declared defaulter by any financial institution not have its business activities suspended and must not be the subject of legal proceedings for any of the foregoing reasons not have, and their directors and officers not have, been convicted of any criminal offence related to their professional conduct or the making of false statements or misrepresentations as to their qualifications to enter into a procurement contract within a period of three years preceding the commencement of the procurement process, or not have been otherwise disqualified pursuant to debarment proceedings not have a conflict of interest in the procurement in question as specified in the bidding document 	Undertaking by the authorized signatory on stamp paper as per format
12	Tender Fee and EMD	Tender Fee and EMD as per RFP terms

Note:

- The Work Order and Work Completion Certificate must be in English language only. In case the Work Order or Work Completion Certificate is in any other language, the bidder must submit notarized Work Order in English language only.
- All above mentioned documents for Pre-Qualification Criteria of bid must be notary-certified true copy/ self-attested.
- The bidders must submit all the supporting documents required along with Technical bid. No new qualifying documents will be entertained. The documents received in the Technical bid will be treated as full and final and evaluation will be carried out accordingly. However, VSCDL reserves the right to seek clarification/documents pertaining to information submitted as a part of the Technical bid.

3.2 OEM Selection Criteria

The OEM Selection criteria for participating in this tender are mentioned in the table below.

#	Criteria	Proof Document Required
1.	OEMs of all proposed equipment/components should have existence in India for last three years as on 31 May 2020	Copy of Certificate of Incorporation of OEM organisation.
2.	The proposed OEM for each of the Cyber security device/solution to be procured under this RFP should have implemented / under implementation in minimum of three organizations in India	Copy of Work Order with Full BoQ of the project from the client/MSI/distributor clearly depicting the solution ordered, brief scope of work and OEM selected for cyber security solution components.

4 Instructions to Bidder

1. Bidders are advised to study all instructions, forms, terms, requirements and other information in the Bid Documents carefully.
2. Submission of bid shall be deemed to have been done after careful study and examination of the Bid Document with full understanding of its implications.
3. The response to this Bid document should be full and complete in all respects. Failure to furnish all information required by the Bid documents or submission of a proposal not substantially responsive to the Bid documents in every respect will be at the bidder's risk and may result in rejection of its proposal.
4. Additionally, proposals of only those bidders who satisfy the Conditions of Eligibility, stated herein, will be considered for evaluation by VSCDL.

Important Clarifications

1. References to “Vendor”, “bidder”, “Bidder”, “SI”, “Service Provider” etc. in this RFP document shall be construed to refer to the Bidder itself.
2. References to “VSCDL”, “VSCDL”, “purchaser”, “buyer”, “customer”, etc. in this RFP document shall be construed to refer to VSCDL (i.e. Vadodara Municipal Corporation or the Smart City SPV, as the case may be).
3. ‘Solution’ means setting up of Cyber Security Operation Centre in VSCDL.
4. “The Project Site” means ICCC and Data Centre of VSCDL located at Badamadi Baug, Vadodara
5. Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, security includes both cyber security and physical security. Ensuring cyber security requires coordinated efforts through an information system. It includes collection of policies, security concepts, security safeguards, guidelines, risk management approaches, tools, training, best practices, assurance and technologies that can be used to protect cyber environment, organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications, systems, and the totality of transmitted and / or stored information in the cyber environment.
6. Cyber Security Operations Center (CSOC), Security Operations Center (SOC) mean bidder providing services for Cyber Security Operations Center (CSOC)
7. SIEM means Security Incident and Event Management
8. DC means VSCDL’s Primary Data Centre at ICCC Building, Badamadi Baug, Vadodara
9. DR, DRS means VSCDL’s Disaster Recovery Centre (site) which currently is at ESDS Nashik.
10. T & C means Terms and Conditions

4.1 Availing Bid Documents

The RFP document can be downloaded from the nprocure Website (vmc.nprocure.com) as well as www.vmc.gov.in www.vadodarasmartcity.in up to the date and time mentioned in the relevant section.

4.2 Completeness of the RFP

Bidders are advised to study all instructions, forms, terms, requirements and other information in the RFP documents carefully. Submission of bid shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications. The response to this RFP should be full and complete in all respects. Failure to furnish all information required by the RFP documents or submission of a proposal not substantially responsive to the RFP documents in every respect will be at the bidder's risk and may result in rejection of its Proposal.

The purpose of this RFP is to provide interested parties with information that may be useful to them in making their financial offers pursuant to this RFP (the "Bid"). This RFP includes statements, which reflect various assumptions and assessments arrived at by the VSCDL in relation to the project. Such assumptions, assessments and statements do not purport to contain all the information that each bidder may require. This RFP may not be appropriate for all persons, and it is not possible for the VSCDL, its employees or advisors to consider the investment objectives, financial situation and particular needs of each party who reads or uses this RFP. The assumptions, assessments, statements and information contained in this RFP, may not be complete, accurate, adequate or correct. Each bidder should, therefore, conduct its own investigations and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements and information contained in this RFP and obtain independent advice from appropriate sources.

VSCDL also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any bidder upon the statements contained in this RFP.

VSCDL may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information, assessment or assumptions contained in this RFP.

The issue of this RFP does not imply that VSCDL is bound to select a bidder or to appoint the successful bidder, as the case may be, for providing digitization services; and VSCDL reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever.

4.3 Proposal Preparation Cost

The bidder is responsible for all costs incurred in connection with participation in this process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings/discussions/presentations, preparation of proposal, in providing any additional information required by VSCDL to facilitate the evaluation process, and in negotiating a definitive Contract or all such activities related to the bid process. VSCDL will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process. All materials submitted by the bidder shall become the property of the VSCDL and may be returned at its sole discretion.

4.4 Pre-Bid Meeting (Virtual)

VSCDL will host a virtual pre-bid meeting for queries (if any) by the prospective bidders. The date, time and place of the meeting are given in Section 2.2. The representatives of the bidders may attend the pre-bid meeting at their own cost. The purpose of the pre-bid meeting is to provide a forum to the bidders to clarify their doubts/seek clarification or additional information, necessary for them to submit their bid.

All enquiries from the bidders relating to this RFP must be submitted to VSCDL's Information & Technology Department. These queries should also be emailed to **smartcity_itcell@vmc.gov.in**. The queries should necessarily be submitted in the following format and **should be in Microsoft Excel only (.xls or .xlsx format). Scanned images and any format (including .pdf format) other than Microsoft Excel will not be accepted.**

Request for Clarification		
Name and Address of the Organization Submitting Request	Name and Designation of Person Submitting Request	Contact Details of the Organization/ Authorized Representative
Organization Name: Address:	Requestor Name: Designation:	Tel: Mobile: Fax: Email:

Sr.	RFP Document Clause/Section Number	Clause Title	Page No	Content of the RFP Requiring Clarification	Clarification Sought
1					
...					

(PDF or scanned images will not be accepted)

Queries submitted post the mentioned deadline or which do not adhere to the above mentioned format may not be responded to. All the responses to the queries (clarifications/corrigendum) shall be made available on (n)Procure (<https://vmc.nprocure.com/>). The date, time of receiving pre-bid queries are given in Section 2.2.

4.5 Conflict of Interest

- A “Conflict of Interest” is any situation that might cause an impartial observer to reasonably question whether Service Provider actions are influenced by considerations of your firm’s interest at the cost of Government. The Service Provider agrees that it shall hold the VSCDL’s interest paramount, without any consideration for future work, and strictly avoid any Conflict of Interest with other assignments of a similar nature. In the event the Service Provider foresees a Conflict of Interest, the Service Provider shall notify VSCDL forthwith and seek its approval prior to entering into any arrangement with a third party which is likely to create a Conflict of Interest.
- Bidders shall not have a conflict of interest that may affect the Selection Process or the scope (the “Conflict of Interest”). Any bidder found to have a Conflict of Interest shall be disqualified.
- VSCDL requires that the bidder provides professional, objective, and impartial advice and at all times hold the VSCDL’s interests paramount, avoid conflicts with other assignments or its own interests, and act without any consideration for future work.
- The Service Provider shall disclose to VSCDL in writing, all actual and potential Conflicts of Interest that exist, arise or may arise (either for the Service Provider or its team) during the term of the Agreement as soon as it becomes aware of such a conflict.

4.6 Amendment of RFP Document

- At any time before the deadline for submission of bids, the VSCDL, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the RFP document by an amendment.
- The bidders are advised to visit the (n)Procure website (<https://vmc.nprocure.com/>) on regular basis for checking necessary updates. VSCDL also reserves the rights to amend the dates mentioned in this RFP for bid process.
- In order to afford prospective bidders reasonable time in which to take the amendment into account in preparing their bids, the VSCDL may, at its discretion, extend the last date for the receipt of bids.

4.7 VSCDL's Rights to Terminate the Selection Process

VSCDL may terminate the RFP process at any time and without assigning any reason. VSCDL makes no commitments, express or implied, that this process will result in a business transaction with anyone. This RFP does not constitute an offer by VSCDL. The bidder's participation in this process may result in VSCDL selecting the bidder to engage in further discussions and negotiations toward execution of a contract. The commencement of such negotiations does not, however, signify a commitment by the VSCDL to execute a contract or to continue negotiations. VSCDL may terminate negotiations at any time without assigning any reason.

4.8 Right to Reject Any Proposal

1. Notwithstanding anything contained in this RFP, VSCDL reserves the right to accept or reject any Proposal and to annul the Selection Process and reject all proposals, at any time without any liability or any obligation for such acceptance, rejection or annulment, and without assigning any reasons therefore.
2. Besides other conditions and terms highlighted in the Tender document, bids may be rejected under following circumstances:

General rejection criteria:

- i. Conditional bids
- ii. If the information provided by the bidder is found to be incorrect/misleading/fraudulent at any stage/time during the tendering process
- iii. Any effort on the part of a bidder to influence the bid evaluation, bid comparison or contract award decisions
- iv. Bids received after the prescribed time and date for receipt of bids
- v. Bids without signature of person (s) duly authorized on required pages of the bid
- vi. Bids without power of attorney/board resolution or its certified true copy

Pre-qualification rejection criteria:

- i. Bidders not complying with the Eligibility Criteria given in this Tender
- ii. Revelation of prices in any form or by any reason before opening the Commercial Bid
- iii. Failure to furnish all information required by the Tender document or submission of a bid not substantially responsive to the Tender document in every respect

Technical rejection criteria:

- i. Technical Bid containing commercial details
- ii. Revelation of prices in any form or by any reason before opening the Commercial Bid

- iii. Failure to furnish all information required by the Tender document or submission of a bid not substantially responsive to the Tender document in every respect
- iv. Bidders not quoting for the complete scope of work as indicated in the Tender documents, addendum/corrigendum (if any) and any subsequent information given to the bidder
- v. Bidders not complying with the Technical and General Terms and conditions as stated in the Tender documents
- vi. Bidders not confirming unconditional acceptance of full responsibility of providing services in accordance with the Scope of Work and Service Level Agreements of this Tender

Commercial rejection criteria:

- i. Incomplete Price Bid
- ii. Price Bids that do not conform to the Tender's Price Bid format
- iii. Total price quoted by the bidder does not include all statutory taxes and levies applicable
- iv. If there is an arithmetic discrepancy in the Commercial Bid calculations the Technical Committee shall rectify the same. If the bidder does not accept the correction of the errors, its bid may be rejected.

Misrepresentation/improper response by the bidder may lead to the disqualification. If such disqualification/rejection occurs after the proposals have been opened and the highest ranking bidder gets disqualified/rejected, then VSCDL reserves the right to consider the next best bidder, or take any other measure as may be deemed fit in the sole discretion of VSCDL, including annulment of the selection process.

4.9 Tender Fee and Earnest Money Deposit (EMD)

1. The bidder should pay non-refundable Tender Fee of INR 10,000/- (Rupees Ten Thousand only) **plus GST**, by Demand Draft in favour of "**Vadodara Smart City Development Limited**", from nationalized or scheduled banks, payable at Vadodara. The Bid Fees shall be in the form of a Demand Draft.
2. The bidder should also pay EMD of INR 20,00,000/- (Twenty Lakhs only) with validity of 180 days from the date of bid submission in favour of "**The CEO, Vadodara Smart City Development Limited (VSCDL)**". It shall be either in form of
 - nationalized/scheduled banks, payable at Vadodara
 - ❖ OR
 - Bank Guarantee issued by Nationalized Bank including IDBI Bank/Private Banks – Axis Bank, HDFC Bank and ICICI Bank along with banks mentioned in the GR of Finance Department of Government of Gujarat (GR No: EMD/10/2015/508/DMO dated 27.04.2016 and its extension Ref: EMD/10/2020/38780/DMO Dated 20th April 2020) only in favour of "The CEO, Vadodara Smart City Development Limited".
3. No interest will be payable by the VSCDL on the Earnest Money Deposit.
4. In case bid is submitted without EMD or Bid Fees as mentioned above then VSCDL reserves the right to reject the bid without providing opportunity for any further correspondence to the bidder concerned.
5. The EMD of unsuccessful bidders will be returned by the Authority, without any interest, as promptly as possible on acceptance of the proposal of the selected bidder or when the Authority cancels the Bidding Process.
6. The selected bidder's EMD will be returned, without any interest, upon the selected bidder signing the Agreement and furnishing the Security Deposit/Performance Guarantee in accordance with the provision thereof.
7. The decision of VSCDL regarding forfeiture of the EMD and rejection of bid shall be final and shall not be called upon question under any circumstances.

8. The EMD may be forfeited:

- If a bidder withdraws their bid or increases their quoted prices during the period of bid validity or its extended period, if any; or
- In the case of a successful bidder, if the bidder fails to sign the Contract or to furnish Performance Bank Guarantee within specified time.
- During the bid process, if a bidder indulges in any such deliberate act as would jeopardize or unnecessarily delay the process of bid evaluation and finalization.
- During the bid process, if any information found wrong/manipulated/hidden in the bid.

VSCDL Bank account details

- Please find below details of VSCDL bank account:
- **Bank:** Bank of Baroda
- **Account number:** 01900100023294
- **Name:** Vadodara smart city development limited
- **IFSC code:** BARBOKHANDE
MICR code: 390012007
Address: khanderao market branch,khanderao market building, rajmahel road,vadodara,baroda,390001
District: Vadodara
- **State:** Gujarat
Branch: khanderao mk branch

Following are the details of the contact person:

- Point of Contact:- Chief Financial Officer, Vadodara Smart City Development Limited
- Email of POC:- smartcitycfo@vmc.gov.in
- Contact number:- 0265-2435646

4.10 Sealing, Marking and Submissions of Bids

Bidders are required to submit their bids in separate sealed envelopes as per instructions given below:

Part 1: Pre-Qualification Bid, Bid Fees, EMD and soft copy in **CD/DVD/Pen drive/USB stick** with complete details as mentioned in Section 10 in “**Envelop 1**” super scribed with Tender No, Due Date and RFP Name – “**Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)**”. The proposal shall also consist with all supporting documents.

Part 2: Technical Bid and soft copy in **CD/DVD/Pen-drive/USB stick** with complete details as mentioned in Section 11 in “**Envelop 2**” super scribed with Tender No, Due Date and RFP Name – “**Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)**”. The proposal shall also consist with all supporting documents, RFP copy, Addendum & Corrigendum, if any.

The large envelope/outer envelope containing above envelopes must be sealed and super-scribed and shall be sent as under:

Details to be mentioned exactly on sealed envelop

<p><u>Tender Details</u></p> <ul style="list-style-type: none"> • Notice No.: ----- • Bid for “Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)”. • Deadline for bid submission: <<DD MMM YYYY>> at <<HH:MM>> 	<p>To,</p> <p>CEO</p> <p>Vadodara Smart City Development Limited</p>
---	--



1. The physical copy of Technical Bid, Tender Fee and EMD must be sent strictly through **Postal Speed Post/Registered Post AD/Courier/In-person** so as to reach on or before the deadline given in the RFP. VSCDL won't be responsible for postal delays.
2. VSCDL will not accept submission of a proposal in any manner other than that specified in the document. Proposals submitted in any other manner shall be treated as defective, invalid and rejected.
3. If the envelopes are not sealed and marked as instructed above, the VSCDL assumes no responsibility for the misplacement or premature opening of the contents of the application and consequent losses, if any suffered by the bidder.
4. Each bidder shall submit only one proposal containing documents as below. A bidder who submits more than one proposal under this contract will be disqualified
 - a. Original Copy of the Tender Fee and EMD
 - b. Pre-qualification Criteria Related Documents
 - c. Technical Proposal Related Documents
 - d. RFP Copy and Addenda & Corrigendum
 - e. The bidder shall prepare original set of the Application (together with originals/copies of documents required to be submitted along therewith pursuant to this document) and applicant shall also provide a soft copy on a Compact Disc (CD)/Pen-drive/USB stick. In the event of any discrepancy between the original and CD/Pen-drive/USB stick, the original shall prevail.
 - f. Each page of the above should bear the initials of the Applicant along with the seal of the Applicant in token of confirmation of having understood the contents. The bid will be signed by the bidder.
5. Pre-qualification and Technical Proposal should be signed by an authorized person of the bidder. The Pre-qualification Proposal should be submitted along with a certified true copy of a board resolution/power of attorney empowering authorized signatory to sign/act/execute documents binding the bidder organization to the terms and conditions detailed in this proposal.
6. Proposals must be direct, concise, and complete. VSCDL will evaluate bidder's proposal based on its clarity and completeness of its response to the requirements of the project as outlined in this RFP. The Chairman, VSCDL or Municipal Commissioner, VSCDL reserves the right to accept or reject any or all the proposals without assigning any reason.

Bid Documents to be uploaded on (n)procure

The Bidder must submit online on (n)Procure website (<https://vmc.nprocure.com/>). Bidder is required to submit the following documents in pdf format (in single file or multiple files):

1. Scan copy of Tender fee and EMD
2. Pre-Qualification Cover letter
3. Table of content page of the PQ physical bid (As per format given in section 9.1)
4. Table of content page of the TQ physical bid (As per format given in section 10.2)
5. Bill of material and BoQ including make, model and quantities offered as per section 10.1.c
6. TQ_4: scan copy for the Undertaking for Manpower deployed on the project
7. Scan copy of the commercial proposal cover letter (As per section 12.1; without prices)

PRICE BID

1. The Price Bid must be submitted online on (n)Procure website (<https://vmc.nprocure.com/>). It should not be sent physically; if submitted physically the bid shall be rejected. Please refer Section 12 for format and instructions.

4.11 Language of Bids

- The bids uploaded by the bidder and all correspondence and documents relating to the bids exchanged by the bidder and VSCDL, shall be written in English language, provided that any printed literature furnished by the bidder in another language shall be accompanied by an English translation in which case, for purposes of interpretation of the bid, the English translation shall govern.
- If any supporting documents submitted are in any language other than English, translation of the same in English language is to be duly attested by the bidder.

4.12 Concessions Permissible under Statutes

Bidder, while quoting against this tender, must take cognizance of all concessions permissible, if any, under the statutes and ensure the same is passed on to VSCDL, failing which it will have to bear extra cost. In case the bidder does not avail concessional rates of levies like customs duty, excise duty, etc. VSCDL will not take responsibility towards this. However, VSCDL may provide necessary assistance, wherever possible, in this regard.

4.13 Bid Validity

The proposal should be valid for acceptance for a minimum period of 180 days from the Bid Opening Date (the "Proposal Validity Period"). If required, VSCDL may request the bidder to have it extended for a further period. The request and the responses thereto shall be made in writing. A bidder agreeing to the request will not be required or permitted to modify his proposal but will be required to extend the validity of EMD for the period of the extension, and in compliance with Clause 4.8 in all respects.

4.14 Firm Prices and Bid Currency

Prices quoted must be firm and final and shall not be subject to any upward modifications, on any account whatsoever. Prices shall be expressed in Indian Rupees (INR) only.

4.15 Right to Vary the Scope of the Work at the Time of Award

VSCDL reserves its right to make changes to the scope of the work at the time of execution of the resultant Agreement. If any such change causes an increase or decrease in the cost of, or the time required for the SI's performance of any part of the work under the Agreement, whether changed or not changed by the order, an equitable adjustment (if required) shall be made in the Contract Value or time schedule, or both, and the Agreement shall accordingly be amended. Any claims by the SI for adjustment under this Clause must be asserted within thirty (30) days from the date of the SI's receipt of the VSCDL changed order.

4.16 Modification or Withdrawal of Bids

1. A bidder wishing to withdraw its bid shall notify VSCDL by e-mail prior to the deadline prescribed for bid submission. A withdrawal notice may also be sent by electronic means such as e-mail, but it must be followed by a signed confirmation copy, postmarked at least one day prior the deadline for submission of bids.

2. The notice of withdrawal shall:

- Be addressed to VSCDL at the address named in the Bid Datasheet,
- Bear the Contract name, the <Title> and <Bid No.>, and the words “Bid Withdrawal Notice.”

3. Bid withdrawal notices received after the bid submission deadline shall be ignored, and the submitted bid shall be deemed to be a validly submitted bid.
4. No bid may be withdrawn in the interval between the bid submission deadline and the expiration of the specified bid validity period. Withdrawal of a bid during this interval may result in the forfeiture of the bidder's EMD.

4.17 Bid Submission Format

The entire proposal shall be strictly as per the format specified in this Request for Proposal. Bids with deviation from this format shall be liable for rejection.

4.18 Documents Comprising of Bids

Following table is provided as the guideline for submitting various important documents along with the bid.

#	Type of Folder	Documents to be submitted
01	Pre-Qualification Folder	<ol style="list-style-type: none"> 1. Bid Covering Letter as per Section 7.1 2. Check-list for the documents for Pre-Qualification Criteria as per Section 7.2 3. Power of attorney/board resolution to the authorized signatory of the bid 4. Scanned copy of payment slip of EMD and Tender Fee 5. Copy of certificate of incorporation 6. Copy of the audited total turnover, turnover from in Information Security projects and profit & loss over last 3 FY (2016-17, 2017-18, 2018-19) As per Section 3.4 7. Certificate from the company secretary/head HR as per Section 3.4 8. Copy of work order and work completion certificate. Cover letter as per Section 8.5 and 8.6 and enclosed copy of Work Order and Work Completion certificate. 9. Copy of registration certificate and number - valid GST registration number. 10. Copy of Income Tax Returns (ITR) for last 3 FY (2015-16, 2016-17, 2017-18) and copy of PAN card 11. Declaration regarding blacklisting as per Section 7.9 12. MAF from OEM(s) authorizing bidder for hardware (server, storage, networking), respective products offered as per Section 8.8 13. Performance Bank Guarantee as per Section 11
02	Technical Proposal Folder	<ol style="list-style-type: none"> 1. Check-list for the documents for Technical-Qualification Criteria as per Section 8.2 2. Technical Proposal 3. Copy of the audited total turnover, turnover from in Information Security projects and profit & loss over last 3 FY (2015-16, 2016-17, 2017-18) as per Section 8.3

		<ol style="list-style-type: none"> 4. Certificate from the Auditor/Company Secretary/Head HR as per Section 8.5. CVs of the proposed resources as per Section 8.7 5. Copy of Work Order and Work Completion Certificate. Cover letter as per Section 8.4 and enclosed copy of Work Order & Work Completion Certificate from the client has to be submitted for the same.
03	Commercial Proposal Folder	<ol style="list-style-type: none"> 1. Commercial Proposal Cover Letter as per Section 9.1. 2. Commercial Bid Formats as per Section 9.2.

Bidders shall furnish the required information on their Pre-Qualification, Technical and Financial Proposals in the enclosed format only. Any deviations in format may make the tender liable for rejection. Disclosure of commercial information of the bid in Pre-Qualification or Technical Envelope shall be sufficient ground for rejection of the bid.

4.19 Evaluation Process

- The bidder must possess the technical know-how and the financial wherewithal that would be required to successfully provide the services sought by VSCDL, for the entire period of the contract. The bidder's bid must be complete in all respect, conform to all the requirements, terms and conditions and specifications as stipulated in the RFP document.
- The evaluation process of the RFP proposed to be adopted by VSCDL is indicated under this clause. The purpose of this clause is only to provide the bidder an idea of the evaluation process that VSCDL may adopt. However, VSCDL reserves the right to modify the evaluation process at any time during the Tender process, without assigning any reason, whatsoever, and without any requirement of intimating the bidder of any such change.
- VSCDL shall appoint a Bid Evaluation Committee (BEC) to scrutinize and evaluate the Technical and Commercial Bids received. The BEC will examine the bids to determine whether they are complete, compliant, and responsive and whether the bid format confirms to the RFP requirements. VSCDL may waive any informality or nonconformity in a bid which does not constitute a material deviation according to VSCDL.
- On opening the Pre-Qualification folder, if it is found that the Bidder has not submitted required documents as per Pre-Qualification folder, then the Bidder shall be given a single opportunity to submit required documents/clarifications within 4 days from the intimation by VSCDL (through email communication mentioning stipulated date), failing which the bid shall be termed as non-responsive.
- On opening the Technical Qualification folder, if it is found that the Bidder has not submitted required documents as per Technical Qualification folder (Packet 'B') then the Bidder shall be given a single opportunity to submit required documents/clarifications within 10 days from the intimation by VSCDL (through email communication mentioning stipulated date), failing which the bid shall be termed as non-responsive.
- There should be no mention of bid prices in any part of the bid other than the Commercial bids.

4.20 Technical-Qualification Criteria and Evaluation of Technical Bids

- The Technical Bids of only those bidders, who qualify in the Pre-Qualification stage, shall be considered and will be evaluated as per the evaluation criteria in this clause. The Bid Evaluation

Committee (BEC) may invite each bidder to make a presentation as part of the technical evaluation.

- **The Demonstration/Presentation will consist of demonstration/pilot the product/solution offered as part of their technical offer, demonstration of test/use cases mentioned in RFP and will consist of the following:**
- The BEC may require written clarifications from the bidders to clarify ambiguities and uncertainties arising out of the evaluation of the bid documents.
- In order to qualify technically, a bid must secure a minimum of 70% of total marks.
- Only those bids which have a minimum score of 70% of total marks will be considered for opening of their Commercial Bid. Only the bids qualifying the technical evaluation will be considered for commercial evaluation.
- Technical evaluation of the bids would be carried out on 5 broad parameters as given below:

Section	Evaluation Criteria	Weightage
A	Bidders Organizational Financial Strength	10%
B	Bidder Experience	15%
C	Project Resources for Deployment	15%
D	Approach & Methodology and Technical Compliance	30%
E	Project Presentation	30%
	Total	100%

#	Technical Evaluation Criteria	Technical Evaluation Parameter	Weightage
A. Organizational Financial Strength			
A1	Organization Financial Strength	Turnover of the bidder- Average annual turnover of Rs.30 Crores in the last three financial years (i.e. 2016-17 & 2017-2018 & 2018-19) from Information Technology business in India <ul style="list-style-type: none"> • 30 to <50 Crore Turnover: 7 marks • 50 to <100 Crore Turnover: 8 marks • 100 to <150 Crore Turnover: 9 marks • > 150 Crore: 10 Marks 	10%
B. Bidder Experience			
B1	Bidder Experience	Total Number of Projects carried for Information Security activities in India in last three years to be submitted by the bidder. (Project value should be at least 5 crores) One mark per assignment /Work Order & Completion Certificate [Max 5 marks]	5%
B2	Bidder Experience	Total Number of Projects executed for IT Governance, IT Assessment or Information Security Policy Implementation in India in last three years to be submitted by the bidder. (Project value	10%

		should be at least Rs. 20 lakhs and at least one project should have been implemented in Government/PSU) Two mark per assignment/ Work Order & Completion Certificate [Max. 10 marks]							
C. Project Resources									
C1	Project Resources for Deployment	Number of employees on permanent payroll having Valid certificates specified in Revised PQ clause Point 4 (Resources with multiple Valid certificates will get one mark) • One mark per resource – Max Mark 15	15%						
D. Approach & Methodology and Technical Compliance									
D1	Approach & Methodology and Technical Compliance	<div>• Following parameters will be evaluated:</div> <table><tr><th>Parameter</th><th>Marks</th></tr><tr><td>Completeness of Project Solution, project plan, Solution Architecture, Approach, Maintenance and Support Plan, SLA Management Plan</td><td>10</td></tr><tr><td>Technical Compliance of the Solution components, Clarity of BoM with unique make and model</td><td>20</td></tr></table>	Parameter	Marks	Completeness of Project Solution, project plan, Solution Architecture, Approach, Maintenance and Support Plan, SLA Management Plan	10	Technical Compliance of the Solution components, Clarity of BoM with unique make and model	20	30%
Parameter	Marks								
Completeness of Project Solution, project plan, Solution Architecture, Approach, Maintenance and Support Plan, SLA Management Plan	10								
Technical Compliance of the Solution components, Clarity of BoM with unique make and model	20								
E. Project Presentation and Demonstration/PoC									
E1	Presentation	<div>Presentation and Demonstration (Please see detailed guidelines below)</div> <table><tr><th>Parameter</th><th>Marks</th></tr><tr><td>Visit or Virtual visit to the project site credential/citations is given in PQ clause 5. If bidder is unable to present the project site for visit, then no marks will be assigned for this parameter.</td><td>15</td></tr><tr><td>POC, Presentation & Demonstration (Vulnerability Analysis/Report)</td><td>15</td></tr></table>	Parameter	Marks	Visit or Virtual visit to the project site credential/citations is given in PQ clause 5. If bidder is unable to present the project site for visit, then no marks will be assigned for this parameter.	15	POC, Presentation & Demonstration (Vulnerability Analysis/Report)	15	30%
Parameter	Marks								
Visit or Virtual visit to the project site credential/citations is given in PQ clause 5. If bidder is unable to present the project site for visit, then no marks will be assigned for this parameter.	15								
POC, Presentation & Demonstration (Vulnerability Analysis/Report)	15								

Evaluation shall be done based on the information provided in the Technical Proposal (and subsequent clarification, if any) and Clarifications/Answers given to the BEC during the presentation by the bidders (if the presentations are held).

4.21 Technical Presentation and Demonstration

- Qualified bidders shall be called for Technical Presentation and Demonstration of their offered solution
- Use cases for the CSOC solution similar to those mentioned in “Functional and Technical Specifications” will be tested and verified in the Demo. The date of the Demo and Bidder presentation, timelines, the final list of use cases, and locations for testing will be shared with all qualified Bidders.
- The Demo and presentation would be rated by VSCDL and scores would be assigned to each demo and presentation.
- The bidder can demonstrate the use cases for proposed solutions either in live environment or through WebEx simulated own sandbox / test environment.

- The qualified Bidders shall be invited to VSCDL to deliver a demo and presentation for maximum of 90 minutes on the solutions that are proposed.
- Score for the demo and presentation exercise will be awarded to the bidder as per the following:
 - a) Proposed Architecture for CSOC
 - b) Approach for implementation for all solutions and services
 - c) Proposed Project Plan
 - d) Resources and Team Structure
 - e) Demonstration of use cases
 - f) Methodologies, Procedures, Tools, Utilities, Templates Developed / used during execution of previous assignments and arrangements for BCPDR Infrastructure proposed etc

The solution demonstration must cover, but not limited to, the following capabilities:

- Threat intelligence
- 24\7 Security monitoring
- Incidence response
- Incident forensics
- Alert triage process
- Incident playbooks
- Alert prioritization matrix
- Incident Categorisation
- Incident security process
- Reporting matrix and KPIs
- Incident Response processes
- Vulnerability identification and remediation

4.22 Opening and Evaluation of Commercial Bid

- VSCDL will open the Commercial Bids of only Technically Qualified Bidders, in the presence of the nodal officer/designated representatives of the bidder who choose to attend, at the time, date and place, as decided and communicated by VSCDL.
- The Commercial Bids will be evaluated by VSCDL for completeness and accuracy. Arithmetical errors will be rectified on the following basis. If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected. If there is a discrepancy between words and figures, the amount in words will prevail.
- The amount stated in the proposal form, adjusted in accordance with the above mentioned procedure, shall be considered as binding, unless it causes the overall proposal price to rise, in which case the proposal price shall govern.
- If the bidder does not accept the correction of errors, its bid will be rejected and the bid security may be forfeited.

4.23 Award Criteria

VSCDL will award the Contract to the bidder based on L1 basis, which means the bidder quoting the minimum amount based on the price bid submitted. No additional cost in any form will be entertained by VSCDL in the contract period. Please refer to commercial evaluation criteria in **Annexure III**.

4.24 Rights to Accept/Reject any or all Proposals

VSCDL reserves the right to accept or reject any proposal, and to annul the bidding process and reject all bids at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the grounds for VSCDLs' action.

4.25 Notifications of Awards and Signing of Contract

- Prior to the expiration of the period of proposal validity, the bidder will be notified in writing or by fax or email that its proposal has been accepted.
- VSCDL shall facilitate signing of the contract within the period of 30 days of the notification of award. However, it is to be noted that the date of commencement of the project and all contractual obligations shall commence from the date of issuance of Purchase Order/Letter of Acceptance, whichever is earlier. All reference timelines as regards the execution of the project and the payments to the Implementation Agency shall be considered as beginning from the date of issuance of the Purchase Order/Letter of Acceptance, whichever is earlier.
- The notification of award (LoI/Purchase Order) will constitute the formation of the Contract. Upon the Bidder's executing the contract with VSCDL, it will promptly notify each unsuccessful bidder and return their EMDs.
- At the time VSCDL notifies the successful bidder that its bid has been accepted, VSCDL will send the bidders the Pro Forma for Contract, incorporating all clauses/agreements between the parties. Within 15 days of receipt of the Contract, the successful bidder shall sign and date the Contract and return it to VSCDL. Draft format of the contract is given in the Annexure VII, Section 13.

4.26 Quantity Variation

- At the time of award of contract, the quantity of goods, works or services originally specified in the bidding documents may be increased or decreased. The successful bidder shall not object to the upward or downward variation in quantities of any item within the variation limit of $\pm 20\%$. *Quantities of central cyber security components (NGFW, WAF etc.) will not have any variation.*
- Repeat orders for extra items or additional quantities may be placed within 2 years of the original request order. The Unit Rate mentioned in the Commercial bid formats shall be used for the purpose of "Repeat Orders" for respective items. However, based on the market trends, VSCDL retains the right to negotiate the Tender rate and/or request better specifications based on market and technological scenario. Delivery or completion period may be proportionally increased.

4.27 Performance Bank Guarantee

- The successful bidder shall at his own expense, deposit with department, within 60 days of the notification of award (done through issuance of the Purchase Order/Letter of Acceptance), an unconditional and irrevocable Performance Bank Guarantee (PBG) from a list of approved banks as per the format given in this Bid document, in favour of VSCDL (VSCDL) for the due performance and fulfilment of the contract by the bidder.
- There will be two Performance Bank Guarantee. One PBG for the implementation phase valid for 1 years, and one PBG for operations phase for 5 years from Go-Live. The implementation phase PBG will be 10% of CAPEX and operations phase PBG will be 10% of OPEX for 5 years. All charges whatsoever such as premium, commission, etc. with respect to the Performance Bank Guarantee shall be borne by the bidder.
- The successful bidder shall maintain a valid and binding Performance Guarantee for a period of three months after the expiry of the Contract Period ("Validity Period").

- The Performance Bank Guarantee letter format can be found in the Annexure VII, Section 13 of this document.
- The Performance Bank Guarantee may be discharged/ returned by department upon being satisfied that there has been due performance of the obligations of the bidder under the contract. However, no interest shall be payable on the Performance Bank Guarantee.
- If the bidder, fails to furnish the Performance Guarantee, it shall be lawful for the Authority to forfeit the EMD and cancel the contract or any part thereof
- In the event of the bidder being unable to service the contract for whatever reason, department would evoke the PBG. Notwithstanding and without prejudice to any rights whatsoever of department under the Contract in the matter, the proceeds of the PBG shall be payable to department as compensation for any loss resulting from the bidder's failure to complete its obligations under the Contract. Department shall notify the bidder in writing of the exercise of its right to receive such compensation within 14 days, indicating the contractual obligation(s) for which the bidder is in default.
- Department shall also be entitled to make recoveries from the bidder's bills, performance bank guarantee, or from any other amount due to him, the equivalent value of any payment made to him due to inadvertence, error, collusion, misconstruction or misstatement.

4.28 Vandalism/Force Majeure

The Bidding Process shall be governed by, and construed in accordance with, the laws of India and the Courts at Vadodara shall have exclusive jurisdiction over all disputes arising under, pursuant to and/or in connection with the Bidding Process.

4.29 Failure to Agree with the Terms & Conditions of the RFP/Contract

Failure of the bidder to agree with the Terms & Conditions of the RFP/Contract shall constitute sufficient grounds for the annulment of the award of Contract, in which event the Contract may be awarded to the next most responsive bidder.

4.30 Terms and Conditions of the Tender

Bidder is required to refer to the draft Contract Agreement, attached as **Annexure VIII** in this RFP, for all the terms and conditions (including project timelines) to be adhered by the successful bidder during Project Implementation and Post Implementation period. Please note that one needs to read the Contract Agreement as a whole document; and the Annexure mentioned there-in may not correspond to the RFP Annexure.

5 Scope of Work

The Scope of work for Implementation of Cyber Security Solutions and Cyber-Security Operation Centre (CSOC) includes but not limited to design, supply, configuration, implementation, customization, integrations, monitor, manage, backup, documentation, training, warranty support, post warranty maintenance support and any other activities related to or connected to the , IT security, Security solutions, devices and technologies as asked in this RFP, viz :

- NG Firewall (External)
- Web Application Firewall solution
- Additional Licenses for Servers
- Additional Licenses for Desktops
- Server Security (HIPS) (For servers)
- DLP Solution (End point, Web, Network, File Share)
- SIEM solution
- Anti APT Solution
- NAC (Network Access Control) Solution
- IDAM Solution
- Cybersecurity Solutions for DR Site
- Integration with existing HSM

5.1 Detailed Scope of Services

The Detailed scope of services shall comprise the following:

The bidder shall carry out the following activities as part of detailed scope of work:

- i. Supply, Installation, Configuration, Commissioning and Maintenance of Cyber Security Components
- ii. Design, implementation and operations of Centralized Security Operations Centre
- iii. Preparation and Implementation of Cyber Security Framework and Policy
- iv. IT infrastructure Review including Vulnerability Assessment and Penetration Testing through Third-Party Cert-In Empanelled Agency
- v. Operation and Maintenance (O&M) for five years contract period post go-live.

The following sections provide details of the activities to be carried out by the bidders as part of the aforementioned scope.

5.1.1 Supply, Installation, Configuration, Commissioning and Maintenance of Cyber Security Components

The bidder shall supply, install, configure, commission and maintain the following cyber security components as part of the overall project scope. The implementation of the cyber security components will be carried out in two phases as per the details provided below:

Phase	S. No.	Item	UOM	Qty.
-------	--------	------	-----	------

Phase-1	1.	NG Firewall (External) (1+1 in HA mode)	Number	2
	2.	Web Application Firewall solution	Lot	1
	3.	Additional AV Licenses for Servers	Number	250
	4.	Additional AV Licenses for Desktops	Number	500
	5.	SIEM solution	Lot	1
	6.	PIM Solution	Lot	1
	7.	Integration with existing HSM	Lot	1
Phase-2	8.	Server Security (HIPS)	Lot	1
	9.	DLP Solution	Lot	1
	10.	Anti APT Solution	Lot	1
	11.	NAC (Network Access Control) Solution	Lot	1
	12.	2 Factor Authentication	Lot	1

The Bidder shall carry out the following activities as part of the supply, installation, configuration, commissioning, operations and management of the security components.

1. Procurement and supply of cyber security components from the respective OEMs/vendors within the stipulated timelines. The MSP can procure the components and tools in a staggered approach based on the implementation plan of components and tools.
2. Installation and configuration of the proposed security components and integration with existing security components comprising of the following key activities:

a. Next Generation Firewalls

- i. The bidder shall install and configure Perimeter Firewalls and Core Firewalls as per their approved To-Be framework at the Data Centre and DR site.
- ii. The bidder shall configure the firewall zones and rules for all network traffic. Rules shall be configured on the basis of source and destination addresses.

b. Web Application Firewall

- i. The bidder shall implement Web Application Firewalls at the Data Centre and DR site and shall be deployed to protect the web applications of e-CTS.
- ii. The bidder shall configure the web applications firewalls to protect the FTA's web applications from targeted threats such as OWASP Top 10 attacks, SANS Top 25 threats, etc.

c. Antivirus

- i. Installation of antivirus software across all 250 servers and 500 desktops of VSCDL
- ii. Configuration of central management console
- iii. Configuration of all antivirus rulesets
- iv. Configuration of antivirus signature update schedule
- v. Configuration of scanning schedule

d. SIEM Solution

- i. Installation of SIEM solution

- ii. Integration of log sources comprising of all network and security devices, servers, applications, endpoints and user logs.
- iii. Configuration of correlation rules and event use-cases
- iv. Configuration of incident types, alerting mechanism and incident management procedure
- v. Configuration of rules for discarding false positives
- vi. Integration with threat intelligence platform and web/social media monitoring tools for additional event correlation.

e. Privileged Identity Management

- i. Installation of PIM solution at Data Centre and DR site
- ii. Definition of super-users, privileged users and privileged accounts for VSCDL
- iii. Configuration of privileges and access rights
- iv. Configuration of user policies and settings
- v. Integration with 2FA tools for user management
- vi. Integration with SIEM for event logging and incident management

f. Integration with Existing HSM

- i. The bidder shall integrate the proposed solutions with existing HSM for secure storage of encryption keys wherever applicable

g. Host Intrusion Prevention System

- i. Installation of HIPS agents across all servers and VMs at the Data Centre
- ii. Configuration of central HIPS console for managing all endpoint agents
- iii. Configuration of HIPS settings
- iv. Configuration of HIPS rules
- v. Configuration of rulesets
- vi. Definition of protected objects and HIPS groups
- vii. Configuration of schedule for updates
- viii. Integration with SIEM for event logging and incident management

h. Data Loss Prevention (DLP)

- i. Installation of DLP solution at Data Centre and DR site
- ii. Data classification and identification of sensitive data
- iii. Configuration of access rules for data
- iv. Configuration of rulesets for transfer of data through network/endpoint/email
- v. Integration with SIEM for event logging and incident management

i. Anti-APT

- i. Installation of Anti-APT and integration with firewalls, IPS, WAF and SIEM solutions
- ii. Configuration of rules that define known origins and file types
- iii. Configuration of sandboxing environment as a replica of actual production environment of VSCDL
- iv. Configuration of rules for file types, scripts and network traffic that shall be moved to sandbox environment

j. Network Access Control

- i. The bidder shall install Network Access Control to provide network device management and AAA services.

- ii. The bidder shall configure authentication, authorization and accounting protocols for device authentication
- iii. The bidder shall configure rules for secure connection of devices to FTA's network
- iv. The bidder shall configure rules for detecting rogue devices.

k. 2FA Solution

- i. Implementation of 2FA for all internal users of VSCDL
- ii. Integration of 2FA with directory services and PIM solution
- iii. Configuration rules for generating authentication factors (OTPs, passcodes, tokens)
- iv. Integration with SIEM for log correlation and event management

l. Integration with Existing Setup

- i. The bidder shall integrate the proposed cyber security components and CSOC with the existing infrastructure present at VSCDL.
- ii. The bidder shall integrate the proposed SIEM with existing IT infrastructure components as well as proposed IT components to get a full view of the IT landscape of VSCDL.

3. Commissioning of the proposed security components: Commissioning of the cyber security infrastructure shall include the following activities:

- a. Power-on test of all proposed security components
- b. Configuration check of the proposed security components
- c. Integration check of the proposed security components with existing Data Centre infrastructure
- d. User acceptance and go-live

4. Operations and Maintenance for a period of 5 years following go-live of the proposed solution: The bidder shall provide adequate resources to manage the proposed cyber security components for a period of 5 years following go-live of the solutions. The broad scope of activities for the bidder during this period shall include:

a. Security Administration and Management Services

The bidder shall be responsible for administration and management of the entire cyber security setup of VSCDL during the operations and maintenance phase of the project. The security administration and management services shall at a minimum comprise of the following:

- i. Preparation of Standard Operating Procedures for cyber security administration and management
- ii. Configuration/Re-configuration of all security components and tools
- iii. Fine-tuning of security components and tools
- iv. Regular hardening and patch management of components of the Data Centre, DR site and CSOC components as per guidelines agreed upon.
- v. IT Security Administration – Manage and monitor safety of information/data
- vi. Reporting security incidents and resolution of the same
- vii. Ensure proactive monitoring, management, maintenance & administration of all security devices and update engine, signatures, and patterns.

- viii. Managing and monitoring of anti-virus, anti-malware, phishing and malware for managed resources.
- ix. Ensuring 100 percent antivirus coverage with patterns not older than the period agreed on any given system
- x. Monitoring centralized pattern distribution (live update) and scan for deficiencies
- xi. Maintaining secure domain policies
- xii. Resolution of calls for security notifications, system alerts, vulnerabilities in hardware/ software and alerting VSCDL on critical and high-risk incidents
- xiii. Ensure patch management is carried out for all security systems and tools
- xiv. Providing root cause analysis for all defined problems including hacking attempts
- xv. Monthly reporting on security incidents and attempts as well as the action taken to thwart the same
- xvi. Maintaining updated documentation of security component details including architecture diagram, policies and configurations
- xvii. Performing periodic review of security configurations for inconsistencies and redundancies against security policy
- xviii. Performing periodic review of security policy and suggest improvements
- xix. Reviewing logs daily of significance such as abnormal traffic, unauthorized penetration attempts, any sign of potential vulnerability, security alerts and responses, and proactive measures in the event a problem is detected
- xx. Coordination with all relevant stakeholders for rapid resolution of every incident/problem within mutually agreed timelines
- xxi. Review of security policies/rules on at-least quarterly basis during first year of O&M and followed by half-yearly review for the subsequent years

b. Administration and Management of Network Security Components

The bidder shall carry out administration and management of all network security components deployed as part of the overall security architecture at the Data Centre and DR site. The bidder shall at a minimum carry out the following activities:

- i. Day-to-day administration of the security devices comprising but not limited to firewalls, WAF, Anti-APT, and NAC devices
- ii. Hardening and firmware updates of all network security devices
- iii. Configuration/re-configuration of all network security devices
- iv. Fine-tuning of network security devices
- v. Half-yearly review of rules and policies implemented across all network security devices
- vi. Preventive maintenance activities on all network security devices
- vii. Manage administrator access/console access to all network security devices and update the same whenever changes occur to privileged users for such devices.

c. Endpoint Security Administration and Management

The bidder shall carry out administration and management of all endpoints within VSCDL. The bidder shall at a minimum carry out the following activities:

- i. Configuration/re-configuration of HIPS and antivirus rules and policies
- ii. Daily checks for signature updates for HIPS and antivirus. Update signatures as and when they are released

d. User Identity and Access Management

The bidder shall be responsible for managing user management through the respective PIM, 2FA and directory services. As part of user management activities, the bidder shall at a minimum carry out the following activities:

- i. Management of user roles, privileges, groups and policies
- ii. Secure storage of passwords and enforcement of password policies
- iii. Enforcement of 2FA at all identified levels
- iv. Addition, deletion, modification of user identities and groups after due approval from VSCDL
- v. Administration, management and monitoring of privileged users
- vi. Administration, management and monitoring of privileged access
- vii. Management of directory services
- viii. Administration and management of role-based access controls

Apart from the aforementioned activities for cyber security component implementation, the bidder is responsible for carrying out the following activities:

1. Smart City IT Asset Management

- VSCDL currently doesn't have automated Asset management tool, bidder can utilise and suggest and offer cost effective/free ITAM tool
- The Bidder shall prepare the information asset register (IAR) for all IT assets deployed in the Smart City. The IAR shall capture criticality, rating, classification, owner and custodian of the Asset.
- The Bidder shall develop and implement an appropriate set of procedures for information labelling and handling in accordance with the classification scheme proposed in the cyber security policy of Smart City.
- This needs to be done in coordination with all the System Integrator/ Vendor of VSCDL ICT projects and the solution to be used should be opensource (no additional cost to VSCDL)

2. Access Control system needs to be done in coordination with the existing project system integrators of VSCDL

- The Bidder shall ensure that users shall be provided single sign on functionality (Active Directory is part of one of the VSCDL project) which is required for the applications and solutions deployed as part of this project. VSCDL has Single sign on functionality as part of ICCC project all others projects are being integrated into this Single Sign On
- Remote access to all Smart City IT users shall be securely managed.

3. Communications and Operations Management

- Bidders must ensure that the IT systems in the cyber security solutions are open, scalable and interoperable.
- Bidders must ensure that cyber security solutions systems are designed in such a way that only authenticated users have access to them. Also, the provision of access has to be routed only through designated applications.
- Bidders must ensure that sensitive data is stored in an encrypted format thereby curtailing the database administrator from reading or modifying the stored sensitive data.
- Bidders must enable for the maintenance of an audit trail to record all the administrator, user level activities including the failed attempts thereby enabling a robust high-level security monitoring of the Smart City security infrastructure.
- The Bidders to coordinate with existing project SI and ensure that the Smart City components – Network elements, Operating system, Applications etc. are in sync and adhere to a singular master clock. Thereby ensuring an appropriate logging/ time stamping of incidents and bolstering smooth operation of the Smart City.
- Bidders must ensure that adequate security controls are deployed against the tampering of log information and unauthorized access to the Smart City infrastructure.
- Cyber security solution architecture should have end-to-end adequate security controls to enforce safety, privacy and integrity of confidential data. Necessary controls must be deployed to protect the integrity of data flowing into the control systems and other critical infrastructure.
- All vendors/OEM of the cyber security solutions to provide self-certification for non-existence of backdoors, undocumented and hard coded accounts, **no data leak to unknown entities via backdoor and no antinational propaganda**
- Bidders must ensure that all the information on security incidents is regularly shared with Indian Computer Emergency Response Team (CERT-In) and NCIIPC (National Critical Information Infrastructure Protection Centre) and their help is sought for appropriate mitigation and recovery from the security incidents.
- Bidders shall ensure that Data encryption is implemented using keys which are not stored in the cloud.
- The bidder shall setup Cyber Security Continuous Monitoring process to monitor - physical environment, External service provider activity etc. to detect potential cyber security incidents.

4. Business Continuity Planning and Disaster Recovery

- The Bidder shall monitor the Disaster Recovery site for the Smart City infrastructure and related IT & OT applications.
- The Bidder shall define Business Continuity and Disaster Recovery plan and will perform the testing on a half yearly basis

5. Awareness Training

- The bidder shall deploy appropriate resources to support periodic awareness training based on latest standards of ISMS. The trainings must focus on educating relevant employees (including privileged users, third party, senior management etc.) on

necessary security practices and processes to be followed in order to maintain the Confidentiality, Integrity and Availability of critical data.

- Cyber security awareness trainings should be provided to different focus groups responsible for the security of ICCC and various projects getting executed by VSCDL

6. Security Controls for DR

The Bidder shall ensure that the DR site of VSCDL IT projects are also included in the cyber security solution implementation. Only Log collector in DR is required. DR is Active -Passive mode. There will be no procurement of cyber security components such as NGFW, NAC etc. for DR locations.

5.1.2 Preparation, implementation and operations of Centralized Security Operations Centre

The bidder shall set up Security Operations Centre to ensure continuous monitoring and manage all kinds of cyber security operations related to Smart City such as Incident Management, Logging and Monitoring, Anti-virus Management, Threat Intelligence Support, Secure Technology Disposal and other cyber security support activities to ensure secured Smart City ecosystem.

The bidder shall at a minimum include the following services as part of SOC:

1. Provide 8x7x365 security management and monitoring services for both Data Centre and DR site. In case of emergency and critical situation bidder need to provide these services during night and odd hours.
2. Provide L1, L2 and L3 support. The bidder should provide the approach and methodology for definition of severity levels and response and resolution timelines for L1, L2 L3 level incidents.
3. The bidder is responsible for integration & interfacing of SIEM with all devices and components within the Data Centre.
4. Advance security monitoring services to detect threats not addressed by traditional defence in depth measure and traditional monitoring solution.
5. Definition of use cases to identify and detect security incidents.
6. Support VSCDL in handling incidents that could involve containment/ eradication/ recovery / root cause analysis
7. Identify the origin of threat, online root cause analysis, mitigation steps and measures to prevent recurrence, utilizing network/ host forensic techniques.
8. The bidder shall monitor, detect and manage incidents for the following minimum set of IT infrastructure security events but not limited to:
 - a. Buffer overflow attacks
 - b. Port & vulnerability scans
 - c. Password cracking
 - d. Worm/virus outbreak
 - e. File access failures
 - f. Unauthorized server/service restarts
 - g. Unauthorized changes to firewall rules
 - h. Unauthorized access to systems
 - i. SQL injection
 - j. Cross site scripting
9. Provide advisory on latest threats, vulnerabilities and patches based on VSCDL's landscape.
10. The bidder shall design the storage and log management services so as to provide the following: Logs should be available for live correlation and analysis for a duration of online 6 months and offline 12 months at any given point in time.

11. Report the identified incidents to respective teams and ensure closure of identified incidents.
12. The incidents shall be reported based on the SLAs defined.
13. Prepare reports and dashboards to present the incident monitoring activities status to top management.
14. Design security monitoring standard operating procedures that are required to be followed for VSCDL.

5.1.3 Preparation and Implementation of Cyber Security Framework and Policy

The bidder shall carry out the following activities as part of scope of Cyber Security Framework and Policy implementation for VSCDL.

1. Smart City Cyber Security Framework

- The Bidder shall develop and implement Cyber Security Framework aimed at building a secure and resilient cyberspace for citizens and stakeholders of Smart City. The Framework shall be designed to protect cyberspace information and infrastructure; build capabilities to prevent and respond to cyber-attacks; and minimize damages through coordinated efforts of institutional structures, people, processes, and technology. Framework shall cover Smart City cyber security architecture with reference to the cyber security framework suggested by National Institute of Standards and Technology (NIST), CSA (Cloud Security Alliance) and ISO27001. Framework shall also comply with MoUD guidelines vide circular K- 1S016/6U2016-SC-1.

2. Smart City Cyber Security Policy

- The Bidder shall prepare and implement Smart City Cyber Security Policy and all the supporting procedures based on the relevant international standards including ISO 27001, MoUD guidelines and CERT-In guidelines.

3. Smart City Cyber Security Governance

- Bidder will perform compressive IT Risk assessment and prepare Risk Treatment Plan for the Smart city. Bidder will update the Risk assessment on a yearly basis.
- Bidder will publish status report to all the stakeholders as agreed during the planning phase.
- The Bidder shall facilitate management reporting in form of dashboard covering Risk Assessment results along with risk treatment plan and timeline to the Smart City management.
- The Bidder shall implement all the controls as identified during the Risk assessment and treatment plan as per the agreed timelines.
- The Bidder shall clearly define Organization structure for Smart City Cyber Security with skilled personnel and adequate representation from Senior Management. The organization structure shall also include the roles and responsibilities of personnel deployed for cyber security of Smart City.
- The Smart City cyber security resources shall be deployed as part of the team during the complete contract period i.e. implementation and operation stage.
- The bidder shall deploy a Single Point of Contact (CISO) who will be responsible for managing the entire security operations of VSCDL smart city. This CISO will be responsible for closing all the points related to Cyber Security issue resolution and coordination with all VSCDL project System Integrators to apply all patches to all IT security devices.

5.1.4 IT infrastructure Review including Vulnerability Assessment and Penetration Testing through Third-Party Cert-In Empanelled Agency (TPA)

The bidder shall carry out IT Infrastructure and Security assessment of the smart city systems implemented at Vadodara (both Data Centre and DR site) through a Cert-In Empanelled Agency. This activity shall be carried out by the TPA prior to implementation of cyber security components and CSOC and yearly during Operations and Maintenance. The selection of TPA would be done in

consultation with VSCDL and final approval and SI should select the TPA, whose final approval is given by VSCDL.

A draft report highlighting the gaps observed and detailed recommendations should be prepared by the TPA and discussed with the management.

Based on the observations shared by the TPA, a complete list of possible remediation measures will be prepared by the TPA and shared to VSCDL and target date of closure will be prepared. The observations and remediation measures shall be shared with the respective Vadodara Smart City system integrators for closure.

The TPA shall carry out the following activities as part of IT infrastructure and security review of the Vadodara Smart City systems:

S. No.	Area	Activities
1.	Audit of Non-SAP Applications	<ul style="list-style-type: none"> Business process review – business rules defined by VSCDL for each process Review of Parameters and security controls <ul style="list-style-type: none"> Parameter settings- One time and continuous monitoring Logical access security – Business user creation Review of rights/privileges granted to groups and users User activity logs, audit trails and exception reports available in the system Admin users and access rights Review of Transaction controls <ul style="list-style-type: none"> Review of workflows implemented in the system Authorisation matrix Maker/Checker for various transactions Input controls Validation against the master data creation Transaction encryption controls Clock synchronization Rule set for alarm generation and transaction reporting Review of Interface controls <ul style="list-style-type: none"> FTP file location and access controls Any other applicable controls basis the integration mechanism adopted Review of change management process should be conducted as per the sampling methodology and should comprise review of the following: <ul style="list-style-type: none"> Policy and procedure for change management Adherence to documented change management process Inventory of changes made to the application Change requests initiated for such changes Approval matrix for authorising the changes Impact analysis of the changes Testing results for the changes Approval for releasing the change in the production Review of incident management process should be conducted as per the sampling methodology and should comprise of the following: <ul style="list-style-type: none"> Policy and procedure for incident management Adherence to documented change management process Incident logging mechanism Incident prioritization Escalation mechanism Monitoring and reporting for parameters such as Incident response time, resolution time, etc.

		<ul style="list-style-type: none"> • Review of logging and monitoring process should be conducted as per the sampling methodology and should comprise of the following: <ul style="list-style-type: none"> ○ Policy and procedure for logging and monitoring ○ Review of Access control, storage mechanism, backup of logs ○ Review mechanism for logs and correlation techniques • Review of user management process should be conducted as per the sampling methodology and should comprise of the following: <ul style="list-style-type: none"> ○ Policies and procedures for account management ○ Account creation, modification and deletion process ○ Account reconciliation process • Review of backup management process should be conducted as per the sampling methodology and should comprise of the following: <ul style="list-style-type: none"> ○ Policies and procedures for backup management ○ Review access control, physical security and integrity of backup data and its storage ○ Review of backup restoration procedure checks ○ Adherence to the policies and procedures • Review of Business Continuity/Disaster Recovery Planning (BCP/DR) process should comprise of the following: <ul style="list-style-type: none"> ○ Approved BCP/DR plan • DR test results
2.	Change Management	<p>Review of change management process should comprise of the following:</p> <ul style="list-style-type: none"> • Policy and procedure for change management • Adherence to documented change management process • Inventory of changes made to the infrastructure • Change request tickets initiated for such changes • Approval matrix for authorising the changes • Impact analysis of the changes • Testing results for the changes • Approval for releasing the change in the production
3.	Incident Management	<p>Review of incident management process should comprise of the following:</p> <ul style="list-style-type: none"> • Policy and procedure for incident management • Adherence to documented incident management process • Compliant logging mechanism • Review the incident tickets as per the sampling methodology defined • Setting up the priority • Escalation mechanism • Monitoring and reporting for parameters such as Incident response time, resolution time, etc.
4.	Asset Management	<p>Review of asset (hardware/software) management process should comprise of the following:</p> <ul style="list-style-type: none"> • Policy and procedure for asset management including guidelines for acquisition of new IT equipment's/systems • Adherence to documented asset management process • Maintenance/Updating of asset registers
5.	Antivirus and Patch Management Process	<p>Review of anti-virus and patch management should comprise of the following:</p> <ul style="list-style-type: none"> • Policy and procedure for Virus management and patch management • Review of Antivirus(AV) and patch management process as per the sampling methodology defined

		<ul style="list-style-type: none"> • Schedule of AV updates and patch updates • Security controls of AV server and patch update servers • AV updates status reports, auditing and logging • Review of AV log review records
6.	Third Party Management	<p>Review of third-party management process should comprise of the following:</p> <ul style="list-style-type: none"> • Verify existence of contracts with current IT service providers for IT contractors, hardware and software maintenance, networks, telephony, etc. • Review the contracts for key parameters such as presence of minimum required service levels, key performance indicators (KPIs), penalties for KPI violations, etc. • Policy and procedure for SLA monitoring • Review SLA monitoring and reporting as per the sampling methodology defined
7.	User Access Management	<p>Review of user access management should comprise of the following:</p> <ul style="list-style-type: none"> • Policies and procedures for account management, end user security policy and user access management • Review of list of users and corresponding user access request form as per the sampling methodology • Review of user access to ensure access rights support the segregation of incompatible functions. • Review of user accounts – system/ default/ generic • Review of records for periodic review of existing users in the system • Review of file system permissions
8.	Backup Management	<p>Review of backup management process should be conducted as per the sampling methodology and should comprise of the following:</p> <ul style="list-style-type: none"> • Policies and procedures for backup management • Review access control, physical security and integrity of backup data and its storage • Review of backup restoration procedure checks • Adherence to the policies and procedures
9.	Training and Awareness Programs	<p>Review of training and awareness program to ensure effective user of IT systems should comprise of the following:</p> <ul style="list-style-type: none"> • Review of induction/trainings programs conducted • Review of process defined for conducting training sessions
10.	Desktop Review	<p>Review of desktops (both connected to network and standalone should comprise of the following:</p> <ul style="list-style-type: none"> • Policy and procedure for desktop management • Review of desktop controls • Review of configuration for all workstations • Review of desktop use policy
11.	Physical Environment Security Management &	<p>The physical and environmental security management review should consist of the following activities:</p> <ul style="list-style-type: none"> • Assessment of vulnerability towards natural calamities • Assessment of any systems and delivery channels not available to end users due to external factors • Fire protection systems, their adequacy and state of readiness • General failure of systems as a whole due to external factors, and the related threat perception • Working environment vis-à-vis adequacy of air conditioning and other infrastructure related setup

		<ul style="list-style-type: none"> Physical security and access control to server room/data centers areas where n/w devices reside Premises management Access card management Other security systems, their adequacy and monitoring Temperature and humidity level monitoring and controls Adherence to provisions of VSCDL's Security Policy
12.	Operating Systems Review	<p>The security controls review for Operating System should comprise of the following:</p> <ul style="list-style-type: none"> Access Management User and group privileges System and user policies Remote access policies Logging mechanism Domain architecture and trust relationships Share permissions and definitions Service packs and hot-fixes System services and applications Policies and procedures that govern its use Patch and Antivirus update Registry settings, including registry security permissions Profiles and log-in scripts
13.	Database Review	<p>The security controls review for database should comprise of the following:</p> <ul style="list-style-type: none"> Access controls and allocation of privileges Usage of privilege accounts Auditing, logging and monitoring DBMS configuration Operating system access and user management Roles allocation Backup and recovery
14.	Review of Network Devices	<p>Review the configuration of switches based on following security controls:</p> <ul style="list-style-type: none"> User authentication and password management Authentication, authorization and account settings Security settings on different management interfaces (physical and logical) SNMP configuration Access controls Use of logging and monitoring Configuration to defy common security attacks like IP spoofing, ICMP redirects Delegation of privileged use in accordance with job function Session management Configuration of VLANs and associated protocol Security Controls around port security, Spanning Tree protocol, VLAN Trunking protocol etc Updated version of IOS / patches <p>Review the configuration of routers based on following security controls:</p> <ul style="list-style-type: none"> User authentication and password management Authentication, authorization and account settings

		<ul style="list-style-type: none"> • Security settings on different management interfaces (physical and logical) • SNMP configuration • Use of logging and monitoring • Configuration to defy common security attacks like IP spoofing, ICMP redirects • Delegation of privileged use in accordance with job function • Routing protocols configured and appropriate security settings • Review of access lists for different network segments (to different outside networks) • Updated version of IOS / patches <p>Review the configuration parameters and rule base of the firewall(s) which include the following controls:</p> <ul style="list-style-type: none"> • Placement of firewall within the network • Policies and rule sets • Authentication, Authorization and accounting • Auditing, logging, monitoring, alerting mechanism • Password control and security controls for administrative / management interfaces • Configuration to defy commonly known security attacks • Configuration of access control and priority of traffic flow • Allowed inbound and outbound services • Service proxies, circuit-level gateways, and packet filters • Surrounding firewall security issues • Domain name services • Router protection and participation in firewall functionality • VPN configuration and encryption • Updated version of OS / patches <p>Review the configurations for the proxy server including following controls:</p> <ul style="list-style-type: none"> • Types and applicability of interfaces configured • Allowed / Denied range of hosts • Review of internal and external interfaces • Access controls and allocation of privileges • Authentication mechanism
15.	Vulnerability Assessment and Penetration Testing	<p>Assess vulnerabilities in the VSCDL's network by conducting the following activities:</p> <ul style="list-style-type: none"> • Scan the ranges of IP / Subnets / devices in order to identify the vulnerabilities • Attempt to determine vulnerability by system and application type • Identify the various threats associated, possible impacts and provide recommendations • Verify all vulnerabilities found during the exploit research phase for false positives and false negatives • Attempt to overload the system using DDoS & DoS and latest attacks
16.	Network Performance Review	<p>An analysis of the performance of the network needs to be carried out to ascertain the ability of the network to meet current and future needs of users and to identify any bottlenecks. Network Performance Audit analysis should include the capacity planning analysis, LAN/WAN link utilization and quality analysis, Existing load pattern for network</p>

		device and Uplink, packet flow performance, Congestion area at various topology layer and traffic pattern analysis.
17.	Network Architecture Review	<p>Network Architecture review should be carried out for security and performance which include the following:</p> <ul style="list-style-type: none"> • Review the appropriate segregation of network into various trusted zones • Review the traffic flow in the network • Review the existing routing policy • Review the route path and table audit • Review of routing protocols and security controls therein • Review the security measures at the entry and exit points of the network • Obtaining information about the architecture and address scheme of the network • Checking Inter-VLAN Routing and Optimization. • Checking of redundancy configurations if any • Routing Protocol Analysis • Analyse protocols used and provide recommendation for improvement • Analysis of load balancing mechanism • Analysis of latency in traffic across various links • Review placement of firewalls and DMZ's • Review access control documentation and configuration • Review logical access to business-critical applications, OS, database, network, physical access
18.	Communications and Operations Management Review	<ul style="list-style-type: none"> • IT systems in the cyber security solutions are open, scalable and interoperable. • only authenticated users have access to the Smart City database. Also, the provision of access has to be routed only through designated applications. • Sensitive data is stored in the Smart City database in an encrypted format thereby curtailing the database administrator from reading or modifying the stored sensitive data. • Smart City architecture should include a VPN solution enabling designated users to access necessary applications and functions from remote applications. • Maintenance of an audit trail to record all the administrator, user level activities including the failed attempts thereby enabling a robust high-level security monitoring of the Smart City security infrastructure. • Smart City components – Network elements, Operating system, Applications etc. are in sync and adhere to a singular master clock. Thereby ensuring an appropriate logging/ time stamping of incidents and bolstering smooth operation of the Smart City. • Adequate security controls are deployed against the tampering of log information and unauthorized access to the Smart City infrastructure such as the data center, IoT device control room etc. • Adequate authentication and role-based access. This can be achieved by utilizing Authentication and privilege management technology thereby controlling the access of data as per user privileges. • • • Adequate security controls to enforce safety, privacy and integrity of confidential data. •

		<ul style="list-style-type: none"> Bidders must ensure that IoT field devices and sensory equipment operating within the Smart City periphery connect only to authorize wireless networks. Secure Wi-Fi guidelines as prescribed by the Department of Telecom must be followed. The wireless layer of the Smart City network is appropriately segmented, bifurcating the network into various trusted zones. Thereby segregating public and utility networks via VPN (Virtual private networks), ensuring that the traffic from internet users is not routed into sensor networks and vice versa. The IoT field devices and sensory equipment deployed in Smart City periphery should have a physical interface disabled after installation. System and Network monitoring should be only performed remotely thereby ensuring local cyber-attacks/ tampering of field devices is curtailed. Appropriate network segregation. The internet facing segment of the data center must incorporate a DMZ (Demilitarized zone), where customer application servers would be located. Predefined ports must be assigned for enabling the communication between the customer application servers and utility application servers to facilitate the access/transfer of data. Smart City applications must be hosted within India and must undergo static and dynamic security testing before deployment. Also, the applications must be periodically (at least once a year) tested for adequate security control. The smart city architecture should have: <ul style="list-style-type: none"> ➤ Automatic and secure firmware updates ➤ Device logging and auditing capabilities Vendor self-certification for non-existence of backdoors, undocumented and hard coded accounts. All the information on security incidents to be regularly shared with Indian Computer Emergency Response Team (CERT-In) and NCIIPC (National Critical Information Infrastructure Protection Centre) and their help to be sought regularly for appropriate mitigation and recovery from the security incidents. Data encryption at rest shall be implemented using departments managed keys, which are not stored in the cloud. The bidder to setup Cyber Security Continuous Monitoring process to monitor - physical environment, External service provider activity etc. to detect potential cyber security incidents.
19.	DR Review Security	<p>The security controls should include the following:</p> <ul style="list-style-type: none"> Periodic secure code review shall be performed for cloud applications. Data encryption at rest / transit depending on sensitivity of data shall be implemented using departments managed keys, which are not stored on the cloud. The CSP will undertake to treat information passed on to them as classified. Such Information will not be communicated / published / advertised by the CSP to any person/organization without the express permission of the Department. CSP shall inform all security breach incidents to Smart City management on real time. CSP shall ensure data confidentiality and mention Sub-contractual risk shall be covered by CSP.

		<ul style="list-style-type: none"> • E-Discovery shall be included as clause in SLA with CSP. It is the process of locating, preserving, collecting, processing, reviewing, and producing Electronically Stored Information (ESI) in the context of or criminal cases/proceedings or investigation. Logging and reporting (e.g., audit trails of all access and the ability to report on key requirements/indicators) must be ensured. • The Law Enforcement Agency as mandated under any law for the time being in force may seek access to information stored on cloud as provided by the Service Provider. The onus shall be on the CSP to perform all due diligence before releasing any such information to any such law enforcement agency. • CSP must ensure location of all data related to smart cities in India only. • The Cloud Service Provider's services offerings shall comply with the audit requirements defined under the terms and conditions of the Provisional Empanelment of the Cloud Service Providers (or STQC /MEITY guidelines. The Audit, Access and Reporting Requirements should be as per the terms and conditions of the Provisional Empanelment of the Cloud Service. • CSP's exit Management Plan shall include - Transition of Managed Services & Migration from the incumbent cloud service provider's environment to the new environment and shall follow all security clauses for smooth transition. • SLA with CSP shall cover performance management & dispute resolution escalation. Guidelines on Service Level Agreement issued by MeitY lists out the critical SLAs for cloud services. • Identification and problem resolution (e.g., helpline, call center, or ticketing system) mechanism must be defined. • Change-management process (e.g., changes such as updates or new services) must be defined. • Appropriate segregation of Virtual Private Cloud (VPC) security rules defined as part of firewall should implement role-based access management, Logging and monitoring. • VPN gateway must be setup to ensure controlled access, appropriate security rules must be employed to encrypt outward data flow, IDS, IPS, API Gateways to be setup and ELB logs to be maintained for any activities and access and exceptions to carried out in the cloud setup, Database logs to be routed as part of the Logging VPC setup. • Digital Certificate shall be implemented for secure access. • Web Application Firewall must be provided, Host IPS must be setup on all the Web servers, Web servers must be configured as per the CIS hardening guidelines and baseline security requirements, logging and monitoring should be enabled. • Application access between hosted Smart City applications shall be segregated, internal infrastructure and external traffic, Role based access must be defined, hardening of database instances as per the CIS baselines configuration guidelines in the cloud setup must be ensured, Logging and monitoring must be enabled. • For SLAs to be used to steer the behaviour of a cloud services provider, imposition of financial penalties is to be incorporated. • Bidder shall monitor Vendor Service level agreement for annual end-to-end service availability of 99.9%. The end to end service agreement should be in place for minimum period of five years form the date of operations of the systems.
--	--	---

During O&M Period, the bidder needs to carry out an internal assessment and VAPT on a yearly basis and submit a report to VSCDL covering the scope of work defined in Section 5.1.4.

5.2 Project Planning & Management

The success of the project depends on the proper project planning and management. The key objective here is to establish a common understanding of the project objectives and outcomes amongst key stakeholders & kickoff the project. Additionally, the team would seek to understand the existing IT environment of VSCDL with the help of interviews and available information.

At the onset, the Service Provider shall plan the project implementation in great details & should provide a micro level view of the tasks & activities that they are going to undertake in consultation with the Department. An indicative list of planning related documentation that the Service Provider should make at the onset is as follows:

- **Audit plan:** A detailed week-wise timeline indicating various activities to be performed along with completion dates and resources required for the same along with the sampling methodology to be adopted.
- **Communication Plan:** Detailed communication plan indicating what form of communication will be utilized for what kinds of meeting along with recipients and frequency.
- **Progress Monitoring Plan:** Detailed Daily, Weekly, Monthly Progress Report formats along with issue escalation format. The format will approved by the department to the successful bidder before start of the project.

5.3 Systems Audit

The systems review for **Non-SAP application** shall comprise of the following:

- Business process review – business rules defined by VSCDL for each process
- Review of Parameters and security controls
 - Parameter settings- One time and continuous monitoring
 - Logical access security – Business user creation
 - Review of rights/privileges granted to groups and users
 - User activity logs, audit trails and exception reports available in the system
 - Admin users and access rights
- Review of Transaction controls
 - Review of workflows implemented in the system
 - Authorisation matrix
 - Maker/Checker for various transactions
 - Input controls
 - Validation against the master data creation
 - Transaction encryption controls
 - Clock synchronization
 - Rule set for alarm generation and transaction reporting
- Review of Interface controls
 - FTP file location and access controls
 - Any other applicable controls basis the integration mechanism adopted
- Review of change management process should be conducted as per the sampling methodology and should comprise review of the following:
 - Policy and procedure for change management
 - Adherence to documented change management process

- Inventory of changes made to the application
 - Change requests initiated for such changes
 - Approval matrix for authorising the changes
 - Impact analysis of the changes
 - Testing results for the changes
 - Approval for releasing the change in the production
- Review of incident management process should be conducted as per the sampling methodology and should comprise of the following:
 - Policy and procedure for incident management
 - Adherence to documented change management process
 - Incident logging mechanism
 - Incident prioritization
 - Escalation mechanism
 - Monitoring and reporting for parameters such as Incident response time, resolution time, etc.
- Review of logging and monitoring process should be conducted as per the sampling methodology and should comprise of the following:
 - Policy and procedure for logging and monitoring
 - Review of Access control, storage mechanism, backup of logs
 - Review mechanism for logs and correlation techniques
- Review of user management process should be conducted as per the sampling methodology and should comprise of the following:
 - Policies and procedures for account management
 - Account creation, modification and deletion process
 - Account reconciliation process
- Review of backup management process should be conducted as per the sampling methodology and should comprise of the following:
 - Policies and procedures for backup management
 - Review access control, physical security and integrity of backup data and its storage
 - Review of backup restoration procedure checks
 - Adherence to the policies and procedures
- Review of Business Continuity/Disaster Recovery Planning (BCP/DR) process should comprise of the following:
 - Approved BCP/DR plan
- DR test results

5.4 Cyber liability insurance

At the end of phase 2 implementation the selected bidder shall insure VSCDL for cyber liability insurance which should cover the following:

- Denial of service (DDoS) attacks or the inability to access websites or systems.
- Unauthorized access to, use of, or tampering with data.
- Unauthorized online transactions

- Phishing and email spoofing
- Identity theft
- Disclosure of confidential data (invasion of privacy).
- Malicious or accidental loss of data or digital assets.
- Introduction of malicious code or viruses.
- Cyber extortion, cyber bullying, terrorism threats, e-extortion
- Personal media injury (defamation, libel, or slander) from electronic content.
- Damage to e-reputation
- Crisis management and public relations expenses.
- Data or system restoration.

The overall limit (sum assured) for cyber liability insurance as above shall be INR 10 crores.

5.5 Review for IT Infrastructure

The bidder shall carry out IT infrastructure security review as part of this project as per description given below

5.5.1 IT Process Review

IT process review is a vital part of any information security audit. The review should be conducted in the following areas to verify the adherence to IT processes during infrastructure management:

5.5.2 Change Management Review

Review of change management process should comprise of the following:

- Policy and procedure for change management
- Adherence to documented change management process
- Inventory of changes made to the infrastructure
- Change request tickets initiated for such changes
- Approval matrix for authorising the changes
- Impact analysis of the changes
- Testing results for the changes
- Approval for releasing the change in the production

5.5.3 Incident Management Review

Review of incident management process should comprise of the following:

- Policy and procedure for incident management
- Adherence to documented incident management process
- Compliant logging mechanism
- Review the incident tickets as per the sampling methodology defined
- Setting up the priority
- Escalation mechanism
- Monitoring and reporting for parameters such as Incident response time, resolution time, etc.

5.5.4 Asset Management Review

Review of asset (hardware/software) management process should comprise of the following:

- Policy and procedure for asset management including guidelines for acquisition of new IT equipments/systems
- Adherence to documented asset management process
- Maintenance/Updating of asset registers

5.5.5 Anti-virus and Patch management process Review

Review of anti-virus and patch management should comprise of the following:

- Policy and procedure for Virus management and patch management
- Review of Antivirus(AV) and patch management process as per the sampling methodology defined
- Schedule of AV updates and patch updates
- Security controls of AV server and patch update servers
- AV updates status reports, auditing and logging
- Review of AV log review records

5.5.6 Third Party management Review

Review of third-party management process should comprise of the following:

- Verify existence of contracts with current IT service providers for IT contractors, hardware and software maintenance, networks, telephony, etc.
- Review the contracts for key parameters such as presence of minimum required service levels, key performance indicators (KPIs), penalties for KPI violations, etc.
- Policy and procedure for SLA monitoring
- Review SLA monitoring and reporting as per the sampling methodology defined

5.5.7 User access management Review

Review of user access management should comprise of the following:

- Policies and procedures for account management, end user security policy and user access management
- Review of list of users and corresponding user access request form as per the sampling methodology
- Review of user access to ensure access rights support the segregation of incompatible functions.
- Review of user accounts – system/ default/ generic
- Review of records for periodic review of existing users in the system
- Review of file system permissions

5.5.8 Backup management Review

Review of backup management process should be conducted as per the sampling methodology and should comprise of the following:

- Policies and procedures for backup management
- Review access control, physical security and integrity of backup data and its storage
- Review of backup restoration procedure checks
- Adherence to the policies and procedures

5.5.9 Training and awareness programs Review

Review of training and awareness program to ensure effective user of IT systems should comprise of the following:

- Review of induction/trainings programs conducted
- Review of process defined for conducting training sessions

5.5.10 Desktop Review

Review of desktops (both connected to network and standalone should comprise of the following:

- Policy and procedure for desktop management
- Review of desktop controls
- Review of configuration for all workstations
- Review of desktop use policy

5.5.11 Physical and Environmental Security management Review

The physical and environmental security management review should consist of the following activities:

- Assessment of vulnerability towards natural calamities
- Assessment of any systems and delivery channels not available to end users due to external factors
- Fire protection systems, their adequacy and state of readiness
- General failure of systems as a whole due to external factors, and the related threat perception
- Working environment vis-à-vis adequacy of air conditioning and other infrastructure related setup
- Physical security and access control to server room/data centers areas where n/w devices reside
- Premises management
- Access card management
- Other security systems, their adequacy and monitoring
- Temperature and humidity level monitoring and controls
- Adherence to provisions of VSCDL's Security Policy

5.5.12 IT Infrastructure Configuration Review

The IT Infrastructure Configuration issues can compromise the desired security level to be maintained in the IT assets. The objective of the review should be to identify configuration vulnerabilities that could be exploited by a malicious entity, the reviews cover as applicable.

5.5.13 Operating Systems Review

The security controls review for Operating System should comprise of the following:

- Access Management
- User and group privileges
- System and user policies
- Remote access policies
- Logging mechanism
- Domain architecture and trust relationships
- Share permissions and definitions
- Service packs and hot-fixes

- System services and applications
- Policies and procedures that govern its use
- Patch and Antivirus update
- Registry settings, including registry security permissions
- Profiles and log-in scripts

5.5.14 Database Review

The security controls review for database should comprise of the following:

- Access controls and allocation of privileges
- Usage of privilege accounts
- Auditing, logging and monitoring
- DBMS configuration
- Operating system access and user management
- Roles allocation
- Backup and recovery

5.5.15 Review of Network Devices

Review the configuration of switches based on following security controls:

- User authentication and password management
- Authentication, authorization and account settings
- Security settings on different management interfaces (physical and logical)
- SNMP configuration
- Access controls
- Use of logging and monitoring
- Configuration to defy common security attacks like IP spoofing, ICMP redirects
- Delegation of privileged use in accordance with job function
- Session management
- Configuration of VLANs and associated protocol
- Security Controls around port security, Spanning Tree protocol, VLAN Trunking protocol etc
- Updated version of IOS / patches

Review the configuration of routers based on following security controls:

- User authentication and password management
- Authentication, authorization and account settings
- Security settings on different management interfaces (physical and logical)
- SNMP configuration
- Use of logging and monitoring
- Configuration to defy common security attacks like IP spoofing, ICMP redirects
- Delegation of privileged use in accordance with job function
- Routing protocols configured and appropriate security settings
- Review of access lists for different network segments (to different outside networks)

- Updated version of IOS / patches

Review the configuration parameters and rule base of the firewall(s) which include the following controls:

- Placement of firewall within the network
- Policies and rule sets
- Authentication, Authorization and accounting
- Auditing, logging, monitoring, alerting mechanism
- Password control and security controls for administrative / management interfaces
- Configuration to defy commonly known security attacks
- Configuration of access control and priority of traffic flow
- Allowed inbound and outbound services
- Service proxies, circuit-level gateways, and packet filters
- Surrounding firewall security issues
- Domain name services
- Router protection and participation in firewall functionality
- VPN configuration and encryption
- Updated version of OS / patches

Review the configurations for the proxy server including following controls:

- Types and applicability of interfaces configured
- Allowed / Denied range of hosts
- Review of internal and external interfaces
- Access controls and allocation of privileges
- Authentication mechanism

5.5.16 Vulnerability Assessment and Penetration Testing

Assess vulnerabilities in the VSCDL's network by conducting the following activities:

- Scan the ranges of IP / Subnets / devices in order to identify the vulnerabilities
- Attempt to determine vulnerability by system and application type
- Identify the various threats associated, possible impacts and provide recommendations
- Verify all vulnerabilities found during the exploit research phase for false positives and false negatives
- Attempt to overload the system using DDoS & DoS and latest attacks

5.5.17 Network Performance Review

An analysis of the performance of the network needs to be carried out to ascertain the ability of the network to meet current and future needs of users and to identify any bottlenecks. Network Performance Audit analysis should include the capacity planning analysis, LAN/WAN link utilization and quality analysis, Existing load pattern for network device and Uplink, packet flow performance, Congestion area at various topology layer and traffic pattern analysis.

5.5.18 Network Architecture Review

Network Architecture review should be carried out for security and performance which include the following:

- Review the appropriate segregation of network into various trusted zones
- Review the traffic flow in the network
- Review the existing routing policy
- Review the route path and table audit
- Review of routing protocols and security controls therein
- Review the security measures at the entry and exit points of the network
- Obtaining information about the architecture and address scheme of the network
- Checking Inter-VLAN Routing and Optimization.
- Checking of redundancy configurations if any
- Routing Protocol Analysis
- Analyze protocols used and provide recommendation for improvement
- Analysis of load balancing mechanism
- Analysis of latency in traffic across various links
- Review placement of firewalls and DMZ's
- Review access control documentation and configuration
- Review logical access to business critical applications, OS, database, network, physical access

A draft report highlighting the gaps observed and detailed recommendations should be prepared and discussed with the management. Upon discussion, management comments and target date of closure for the observations should be captured from the management.

5.6 Professional Project Management

Service Provider shall execute the project with complete professionalism and full commitment to the scope of work and the prescribed service levels. Service Provider shall attend regular Project Review Meetings called by VSCDL and shall adhere to the directions given during the meeting. Following responsibilities are to be executed by the Service Provider in regular manner to ensure the proper management of the project:

- Finalization of the Project plan in consultation with VSCDL and its consultant. Project Plan should consist of work plan, communication matrix, timelines, Quality Plan, Configuration Management Plan, etc.
- Plan and deploy the resources in conjunction with the Project Plan and to execute roles and responsibilities against each activity of the project plan
- Submission of Weekly Project Progress Reports

5.7 Use & Acquisition of Assets during the term

The Service Provider shall -

- a) Take all reasonable & proper care of the entire hardware & software, network or any other information technology infrastructure components used for the project & other facilities leased/owned by the Service Provider exclusively in terms of the delivery of the services as per this CA (hereinafter the “Assets”) in proportion to their use & control of such Assets which will include all upgrades/enhancements & improvements to meet the needs of the project arising from time to time.

- b) Term “Assets” also refers to all the hardware / Software / furniture / data / documentations / manuals / catalogues / brochures / or any other material procured, created or utilized by the SERVICE PROVIDER or VSCDL for implementation of cloud-based Enterprise E-mail.
- c) Keep all the tangible Assets in good & serviceable condition (reasonable wear & tear excepted) &/or the intangible Assets suitably upgraded subject to the relevant standards as stated in of the Bid Document to meet the SLAs mentioned in the contract & during the entire term of the Agreement.
- d) Ensure that any instructions or manuals supplied by the manufacturer of the Assets for use of Assets & which are provided to the Service Provider will be followed by the Service Provider & any person who will be responsible for the use of the Asset.
- e) Take such steps as may be recommended by the manufacturer of the Assets & notified to the Service Provider or as may be necessary to use the Assets in a safe manner.
- f) To the extent that the Assets are under the control of the Service Provider, keep the Assets suitably housed & in conformity with any statutory requirements from time to time applicable to them.
- g) Not, knowingly or negligently use or permit any of the Assets to be used in contravention of any statutory provisions or regulation or in any way contrary to law.
- h) Use the Assets exclusively for the purpose of providing the Services as defined in the contract.
- i) Service Provider shall not use VSCDL data to provide services for the benefit of any third party, as a service bureau or in any other manner
- j) Service provider does not acquire implicit access rights to the information or rights to redistribute the information. Any information of VSCDL must be protected by the successful Bidder from unauthorized disclosure, modification or access. The Bidder understands that civil, criminal, or administrative penalties may apply for failure to protect information appropriately. VSCDL decision will be final.

5.8 Security and safety

- a) The Service Provider will comply with the directions issued from time to time by VSCDL and the standards related to the security and safety in so far as it applies to the provision of the Services.
- b) Service Provider shall also comply with VSCDL / Government of Gujarat’s / Government of India’s Information Technology security and standard policies in force from time to time as applicable.
- c) Service Provider shall use reasonable endeavors to report forthwith in writing to all the partners / contractors about the civil and criminal liabilities accruing due to by unauthorized access (including unauthorized persons who are employees of any Party) or interference with VSCDL's data, facilities or Confidential Information.
- d) The Service Provider shall upon reasonable request by VSCDL or his/her nominee(s) participate in regular meetings when safety and information technology security matters are reviewed.
- e) Service Provider shall promptly report in writing to VSCDL any act or omission which they are aware that could have an adverse effect on the proper conduct of safety and information technology security at VSCDL.

6 Functional and Technical Requirements

Proposed Cyber Security Solutions should be fully compliant to MoUD guidelines (*Circular reference number K-15016/6U2016-SC-I*) and the people, process & technology deployed should be provisioned accordingly.

6.1 Security Information and Event Management (SIEM)

The SIEM solution is required to collect logs from network devices, servers, application security logs, Anti-virus, Proxy server, access control system, Cyber Security solutions like Anti-APT, WAF, NAC, other tool etc. In addition, the logs being generated by the solutions deployed as part of the CSOC implementation need to be collected by the SIEM. The bidder should perform the following as part of the SIEM.

A. Solution Implementation:

- a) Implement the SIEM tool to collect logs from the identified devices / applications / databases etc.
- b) Provide and/or develop parsing rules for standard/ non-standard logs respectively.
- c) Implement correlation rules based on out-of-box functionality of the SIEM solution and also based on the use-cases defined.
- d) Inbuilt incident management and ticketing tool to generate tickets for the alert events generated by the SIEM or Separate tool which have capabilities of seamless integration. The tool should have feature to populate the relevant incident details from the alerts into the ticketing tool.
- e) Build custom interfaces/ Connector for Applications. To begin with VSCDL will start with integration of critical applications. Bidders can be asked for integrating further more applications if found critical and required by VSCDL.
- f) While, it is expected that connectors for all the standard applications and devices will be readily available with the Bidder and connector for mostly in-house/custom built applications will need to be developed. Bidder team deployed for CSOC operations will be expected to develop connector for the custom built applications specifically developed for VSCDL.
- g) The SIEM should be able to collect logs from the devices/applications/databases etc. mentioned by VSCDL as per the Annexure X including the solutions deployed as part of this RFP. It should be able to collect the logs from devices from geographically dispersed locations.
- h) For establishment of CSOC, VSCDL will provide Two (2) 60" Inch+ LEDs which will be used to display the configured correlation alerts maintained at the CSOC.
- i) In addition, VSCDL will also provide Four (4) desktops with dual VGA cards/ dual monitors and a minimum of 8 GB RAM and 1 TB HDD for the CSOC monitoring team.
- j) The logs collected by the SIEM log collector should be replicated across primary Data Center and Disaster Recovery location. The bidder will be responsible for providing P2P link for the log replication collected by SIEM log collectors across primary DC site and DR site. The sizing and requirement of all such links will be the responsibility of bidder.
- k) The bidder should provide SIEM license for 10000 EPS from day 1.
- l) Selected Bidder will customize incident management / dashboard / reports for the VSCDL and will modify the same as per the changing requirement of the VSCDL.

- m) Bidder will also supply all the necessary Switches / cables / connectors / hardware /software etc. for integration of the components supplied for CSOC. VSCDL will supply only the Rack space, power and a network point in the Server room.

B. Storage

- a) The SIEM should be able to maintain 3 months of logs on-box. In addition, the bidder should provide for near line storage i.e. secondary storage for archiving logs for up to 9 months and offline storage for storage of logs for up to 5 years. Total 6 years log must be available. The bidder is responsible for sizing the storage adequately based on the EPS of 10,000.
- b)
- c) The Existing tape library of the ICCC project (Installed in Smart DC) needs to be used for StorageThe bidder is responsible for automated online replication of logs from DC to DR for redundancy. The solution should be capable of automatically moving the logs from device to archival storage based on the ageing of the logs. The storage should have “Write Once Read Many (WORM)” / Encryption/ Index and Search/ Retention and Disposal functionality. The storage should have the option to support backup on tape library. For DC-DR replication, the solution should also have the capabilities to replicate the logs in real-time and should have configuration for scheduled replication whenever required. Two WORM drives are required: one at DC and one at DR.
- d) For all data log/storage requirement VSCDL will provide storage space/partition on ICCC storage solution HPE 3PAR 8440. The bidder has to estimate the storage required for such purpose for 7 years and mention the same in technical bid.
- e) VSCDL will provide the storage safe and tape cartridges.
- f) The bidder will have to make the archival logs (secondary storage) available within 24 hours and live logs in real time of a request made by the VSCDL. This request for retrieval of archival logs would be considered as a Medium Priority incident. If the bidder fails to provide the required logs within 24 hours, then penalties applicable for Medium Priority incidents would be levied.

C. Log collection

Logs from all the in-scope devices and additional devices integrated as part of contract period located at the geographically dispersed location should be collected. Bidder / Vendor should develop the baseline for the level of logs to be enabled from different components of IT infrastructure assets. The log baseline should be in line with global best practices. In case the systems/applications are writing logs to the local hard disks, solution should be capable to pull the logs from these devices through secure transfer. Only in case where remote log collection is not feasible, bidder / vendor should install agent on the servers and applications for collection of logs. Raw logs should be made available in case of legal requirement.

D. Log correlation

Collected Logs should be correlated according to various predefined criteria for generation of alert and identification of the incident. The correlation rules should be predefined and also user configurable. Correlation rules should be customized by the bidder on regular basis to reduce false positives. In any case false negatives will not be permitted. In case of detection of any such incident, correlation rules must be customized immediately to capture such incidents.

E. Alert generation

Solution should be capable to generate alerts, register and send/receive the same through message formats like SMTP, SMS, Syslog, and SNMP as per user configurable parameters.

F. Event viewer / dashboard / reports / incident management

SIEM Solution should provide web based facility to view security events and security posture of the VSCDL's Network and register incidents. Solution should have drill down capability to view deep inside the attack and analyze the attack pattern. Dash board should have filtering capability to view events based on various criteria like geographical location, Device type, attack type etc. Dashboard should have Role based as well as Discretionary access control facility to restrict access to incidents based on user security clearance level. Solution should provide various reports based on user configurable parameters and standard compliance reports like ISO27001, IT Act and regulatory reports. Selected bidder will customize incident management / dashboard / reports for the VSCDL and will modify the same as per the changing requirement of the VSCDL.

G. Incident management tool

- a) The principal goal of the incident management process is to identify anomalous activities in the environment, contain those events and restore normal service operation as quickly as possible and minimize adverse impact on business operations, thus facilitating continued service quality and availability.
- b) Solution should be able to register any security event and generate trouble ticket.
- c) Solution should provide complete life cycle management (work flow) of trouble tickets from incident generation till closure of the incident.
- d) Solution should also provide a detailed process for managing incidents - describing each phases of the process – prepare, identify, contain, eradicate/remediate, recover and learn from the incidents responded to.
- e) Solution should provide the logging facility to different levels of users to monitor and manage the incidents generated for closure of the same as per the defined workflow.
- f) Solution should be able to integrate with different tools such as SIEM tool, Vulnerability Management tool etc. Incident management should include escalation as per the escalation matrix. However, it is preferred that the SIEM should have an inbuilt integrated incident management tool.
- g) Detected incidents - Upon receiving an incident record identified by the VSCDL, a Bidder's Security Engineer is assigned to proceed with incident diagnosis and troubleshooting.
- h) Notifications - The Notification Matrix defines the VSCDL's contacts, the incident management process step (initial, diagnose, update and resolve), the method (telephone, mobile, SMS, email) and hours (business hours or after hours). The Notification Matrix shall be customizable as per configuration item. SMS and email Gateway API will be provided by VSCDL
- i) Develop workflow for incident management tool and be responsible for end to end incident management lifecycle.

6.2 Cyber Security Solution Components

Following are the minimum-security solutions/components to be proposed by the bidders as part of the solution. The sizing and the capacity of the equipment should commensurate to the overall business requirement and

technical solutions proposed. Security solutions deployed at different layers should not be provisioned from the same vendor and solutions shall support digital certificate for authentication wherever applicable.

A. NGFW – Next Generation Firewall (External Firewall)

1. The NGFW shall be deployed as external firewall in HA (High Availability) mode. NGFW should support Active/Active and Active/Passive HA mode and must support synchronization of Sessions.
2. Proposed solution should have user authentication capabilities.
3. Management and logging at NGFW shall be securely managed centrally in house. Management Server must support backup with all configuration, certificates etc.
4. Policy Management should have option to create various Layered policy for various Zones.
5. Network Security NGFW should support “Stateful” policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc.
6. Proposed solution must failover without dropping any connection in active-active mode.
7. It should support the IPSec VPN for both Site-Site & Remote Access VPN.

B. WAF – Web Application Firewall

1. Solution should be deployed and protect the web applications from attacks. WAF solution should filter the HTTP/S traffic based on the rules set defined.
2. Proposed solution shall prevent the following attacks (but not limited to): Brute force, Access to predictable resource locations, Unauthorized navigation, HTTP request format and limitation violations (size, unknown method, etc.) and File upload violations
3. Solution should be able to inspect web application output and respond (allow, block, mask and/or alert) based on the active policy or rules, and log actions taken.
4. Support dynamic source IP blocking and should be able to block attacks based on IP source.
5. Support automatic updates (if required) to the signature database, ensuring complete protection against the latest application threats.
6. Integrate with the proposed SIEM solution
7. . Proposed solution should have integrated load balancing for Web application traffic.

C. IDAM – Identity Access Management

1. Solution should provide the ability to make real-time course-grained authorization decisions such as a whether to grant access to an application.
2. Solution should provide the configurable ability to restrict or allow concurrent logins by the same user.
3. Solution should deny assignment of one role to a user, based on their existing role assignment (mutually exclusive roles).
4. Solution should support disablement/deletion of unused or expired accounts
5. Solution should provide a clear audit log of “impersonation” events to enable investigation of who has performed the functions or changed data using an external user’s account
6. Solution should be able to connect to various applications with independent databases so as to include all user profiles from those applications.
7. Solution should perform basic audit and logging capabilities.
8. Solution should aid in documenting clearly all systems access in a global repository, to make it easier to terminate access in the future.
9. Solution should support existing IT Compliance reporting for User Access Verification by periodically auditing the account setup on each system, to measure compliance with standards.
10. Solution shall enforce strong password management features

D. 2FA – Two-Factor Authentication

1. Proposed two-factor authentication system shall ensure remote user-identification.
2. Shall support unlimited number of LDAP servers.
3. Shall support both software and hardware tokens.
4. Proposed solution shall support Active Directory integration
5. Availability as an on premise solution OR MPS-hosted (cloud service).
6. The second factor of authentications will be on SMS as well as Email. VSCDL will provide API for SMS & Email Gateway.

E. PIM – Privileged Identity Management Solution

1. The proposed solution Should support multi factor authentication for privileged users
2. The proposed solution should be able to provide time based sessions for privilege users

3. The proposed solution should support denial of access protection by blocking repeated password failures on multiple administrator accounts in the directory.
4. The proposed solution should enforce segregation of duties as defined in the cyber security policy.
5. The proposed solution should be able to develop privileged identity management audit reports for management.

F. Antivirus Protection

1. The proposed solution should scan files and identifies infections based on behavioural characteristic of viruses
2. The proposed solution should be able to record critical endpoint data- even while devices are offline or outside your corporate network to quickly detect infected systems
3. The proposed solution should provide real time active protection.
4. . The proposed solution should auto-quarantine virus and malware infected files without end-user interaction
5. The proposed solution should have ability to quarantine undetonated malicious executables within the environment with the ability to hunt for such malicious executables
6. The solution should provide the capabilities to log administrative activities such as changes to policies, agent override activities, agent termination and agent uninstall key generation in the management console.

G. DLP – Data Leakage Prevention

1. *DLP for Endpoints* – Proposed solution should address the risks associated with the storage and use of confidential /sensitive data on laptops and desktops across organization. It should prevent confidential/sensitive files from downloading, copying to removable media. Proposed solution should monitor data being copied and pasted from the clipboard to prevent confidential/sensitive data from being pasted to specific application.
2. *DLP for Web* – Proposed solution must block or remove sensitive data from outbound web communications if they violate security policy.
3. *DLP for Network* – Proposed solution must passively inspect network traffic for confidential data that is being sent in violation of security policy.
4. *DLP for Files shares, Databases and Document Repositories (Storage)* – Proposed solution must discover stored confidential data throughout the enterprise; monitor the ownership and use of stored data; and protect sensitive data according to centrally administered policies.
5. Proposed solution is expected to be deployed in HA (High Availability) mode.

H. Server Security (Host Intrusion Prevention System)

1. Proposed solution should protect against Distributed DoS attack and Solution should have the ability to lock down a computer (prevent all communication) except with management server.
2. It should provide automatic recommendations against existing vulnerabilities
3. Solution should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, dns, etc.) and support custom rules as well.
4. Solution should have feature to take backup of infected files and restoring the same.
5. Host IPS should be capable of recommending rules based on vulnerabilities with the help of virtual patching and should have capabilities to schedule recommendation scan and entire features of solution should be agentless.

I. NAC - Network Access Control Solution

1. Proposed solution should be deployed in HA (High Availability) mode.
2. The solution should support continuous detection of devices attempting to connect to the network
3. The solution should be able to integrate with existing directory services/ identity and access management system for Role-based access facility.
4. The solution should be able to report violations based on VSCDL's defined device baseline to the SIEM.
5. The solution should capture audit logs.
6. The solution should be able to detect endpoint Mac address, IP addresses, network resources devices, resources such as printers and scanners, network zones etc. through auto discovery.
7. The solution should be able to identify and authenticate VPN users.

J. SIEM - Security Information & Event Management

1. The SIEM solution is expected to collect logs from security and network devices, servers and application security logs.
2. The proposed solution must have an automated backup and manual recovery process.
3. In the proposed solution, all logs should be Authenticated (time-stamped across multiple time zones) encrypted and compressed before transmission.
4. The proposed solution should provide time based, criticality-based store and forward feature
5. The proposed solution should have the ability to gather information on real time threats and zero day attacks issued by anti-virus vendors or audit logs and add this information as intelligence feed in to the SIEM solution via patches or live feeds
6. The proposed solution should generate the following reports (but not restricted to): User activity reports, Configuration change reports, Incident tracking report, Attack source reports etc. In addition, the proposed solution should have a reporting writing tool for development of any ad-hoc reports.
7. The proposed solution should provide the ability to monitor and alert on non-compliance events in real-time and provide necessary reports and dashboards. Dashboard should support reporting for consolidated relevant compliance across all major standards and regulatory requirements.
8. The proposed solution should have a mechanism to track security incidents across a wide range of relevant attributes (i.e. IP addresses, usernames, MAC address, log source, correlation rules, user defined, etc.).
9. The proposed solution should be possible to define purging and retention rules for log storage. Purging duration and frequency will be decided at the time of System Study and Security Policy Finalisation.
10. The proposed solution should support creation of automated incident management workflows to track incident from creation to closure, provide reports on pending incidents. It should also permit upload of related evidences such as screenshots etc.
11. The proposed Solution must support unlimited devices, flows integration and should have unlimited user license. Must include software licenses for all project landscape (at DC & DR) mentioned in this RFP.

K. Anti -APT

1. Solution must be custom built Anti-APT solution and must not have network perimeter security component part devices like firewall/UTM and IDS/IPS
2. The proposed solution should able to work with the existing technologies for advance threat protection
3. The proposed solution should support to monitor traffic from multiple segments.
4. The proposed solution should have capabilities to configure files, IP, URLs and Domains to Black list or white list.
5. The Proposed solution must provide a web service interface/API for customer to customize integration.
6. The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal.
7. The proposed solution must be able to provide intelligence portal for malware information, threat profile and containment remediation recommendations where applicable.

6.2.1 Next Generation Firewall (NGFW)

S.No	Technical Requirement	Compliance (Y/N)
1	Network Security NGFW should support “Stateful” policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc.	
2	NGFW (Firewall, IPS and application control) should support for Active – Active connections.	
3	Licensing should be a per device and not user/IP based (should support unlimited users)	

RFP for Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL
(Second Attempt)

4	NGFW should support the multicast protocols like IGMP and PIM-DM / PIM-SM	
5	Firewall should support Active/Active and Active/Passive HA mode and must support synchronization of Sessions.	
6	Appliance should have user authentication Capabilities	
7	solution must failover without dropping any connection in active active mode.	
8	The platform should support VLAN tagging (IEEE 802.1q)	
9	Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously	
10	NGFW should support IPv4 & IPv6 static routing, RIP, OSPF v2 & v3, PBR, BGPv4 or BGPv6	
11	Device must support automatic search, downloading and install software hotfixes with minimal administrator efforts	
12	The solution Should support Non-Stop Forwarding in HA during failover and Graceful Restart	
13	Firewall should support Nat of IPv4 and IPv6 addresses	
14	It should support the VOIP traffic filtering	
Hardware and Interface Requirements		
1	The platform must be supplied with at least 6 nos. of GE RJ45, 4xGE SFP interfaces from Day one, and should have option to upgrade 4 x 1G & 2x10G ports in future.	
2	This requirement is optional. If the appliance doesn't have internal harddisk, then the such disk space can be part of separate reporting and logging VM.	
Performance Requirements		
1	NGFW (IPS (Bi-Directional Scan) + Application Control+ Firewall features enabled) Throughput must be minimum 2.5 Gbps. The bidder shall submit the performance test report from Global Product Engineering department or Global Testing/POC Dept or submit technical data sheet and website URL which is available on OEM Global website	
2	The proposed solution must support at least 1 Gbps of VPN throughput. The bidder shall submit the performance test report from Global Product Engineering department or Global Testing/POC Dept or submit technical data sheet and website URL which is available on OEM Global website	
3	The Proposed NGFW appliance must have minimum 50,000 Connection per second.	
4	The Proposed NGFW appliance must support 3 Million Concurrent connection from day one	

Architecture Features		
1	It should support the IPSec VPN for both Site-Site & Remote Access VPN	
2	NGFW system should support IPsec VPN	
Solution Filtering Requirements		
1	It should support the filtering of TCP/IP based applications with standard TCP/UDP ports or deployed with customs ports	
2	The NGFW must not have any limit to define Address objects, if such limit exists than it should support more than 20,000 address objects. OR The NGFW must support Reusable system object definitions for networks, services, hosts, time periods, users and groups, clients and servers.	
3	The NGFW should allow multiple firewall policies/rules	
4	NGFW updates should have an option of Automatic downloads and scheduled/manual updates.	
5	NGFW should support minimum 3000 applications	
6	It should be able to block Instant Messaging like Yahoo, MSN, ICQ, Skype (SSL and HTTP tunneled)	
7	It should enable blocking of Peer-Peer applications, like Kazaa, Gnutella, Bit Torrent, IRC (over HTTP)	
8	The NGFW should support authentication protocols like LDAP, RADIUS and have support for RADIUS or TACACS+ authentication servers.	
9	The NGFW should support advanced NAT capabilities.	
10	NGFW Should support Identity Access for Granular user, group and machine-based visibility and policy enforcement	
Management & Logging		
1	NGFW Appliance should have management console/dashboard/, reporting and logging functionality	
2	NGFW should support role based administration with customised profile for different Admin.	
3	NGFW should support API for third party integration (with the SIEM solution being offered as part of cyber security stack via syslog integration or equivalent)	
4	management Server must support backup with all configuration, certificates etc.	
5	NGFW Management should have Log storage of minimum 1TB HDD internal or external	
6	Firewall should support management of firewall policies via GUI management interface.	

7	Firewall should support the functionality of Auto-Update to check for latest software versions & download the same.	
---	---	--

6.2.2 Web Application Firewall (WAF)

S. No	Technical Requirement	Compliance (Y/N)
1	The proposed solution should be deployed in High Availability with Active-Active/Active-Passive Scenario and should support different deployment modes such as: Inline Transparent, Reverse proxy, Full Proxy..	
2	The proposed solution should be deployed in High Availability with Active-Active/Active-Passive Scenario..	
3	The proposed solution should address Open Web Application Security Project (OWASP) Top Ten security vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), Broken Authentication and Session Management.	
4	The proposed solution should prevent the following attacks (but not limited to): Brute force Access to predictable resource locations Unauthorized navigation Web server reconnaissance HTTP request format and limitation violations (size, unknown method, etc.) Use of revoked or expired client certificate Malicious File upload violations	
5	The proposed solution should have DLP features to identify and block sensitive information such as credit card numbers, PAN Numbers, Aadhar Numbers	
6	The proposed solution should support positive and negative security model	
7	The proposed solution should have out of the box database of signatures for known attacks.	
8	The proposed solution should have the ability of caching, compression of web content and SSL acceleration.	
9	The proposed solution should have integrated SSL Offloading capabilities, further the solution should support SSL and/or TLS termination, or be positioned such that encrypted transmissions are decrypted before being inspected by the WAF.	
10	The proposed solution should meet all applicable PCI DSS requirements pertaining to system components in the cardholder data environment, should also monitor traffic carrying personal information	
11	The proposed solution should allow signatures to be modified or added by the administrator	

12	Should have the ability to inspect web application output and respond (allow, block, mask and/or alert) based on the active policy or rules, and log actions taken.	
13	Should inspect both web page content, such as Hypertext Markup Language (HTML), Dynamic HTML (DHTML), and Cascading Style Sheets (CSS), and the underlying protocols that deliver content, such as Hypertext Transport Protocol (HTTP) and Hypertext Transport Protocol over SSL (HTTPS). (In addition to SSL, HTTPS includes Hypertext Transport Protocol over TLS.)	
14	The proposed solution should support dynamic source IP blocking and should be able to block attacks based on IP source	
15	Should inspect Simple Object Access Protocol (SOAP) and extensible Markup Language (XML), both document- and RPC-oriented models, in addition to HTTP (HTTP headers, form fields, and the HTTP body).	
16	Actions taken by WAF to prevent malicious activity should include the ability to drop requests and responses, block the TCP session, block the application user, or block the IP address.	
17	Transactions with content matching known attack signatures and heuristics based should be blocked.	
18	The proposed solution database should include a preconfigured comprehensive list of attack signatures.	
19	The proposed solution should allow signatures to be modified or added by the administrator.	
20	The proposed solution should support automatic updates (if required) to the signature database, ensuring complete protection against the latest application threats.	
21	The proposed solution should be able to restrict traffic both on the basis of number of files in a request and the size of the file in a request.	
22	WAF support the following normalization methods:	
	URL-decoding (e.g. %XX)	
	Null byte string termination	
	Self-referencing paths (i.e. use of /. / and encoded equivalents)	
	Path back-references (i.e. use of /.../ and encoded equivalents)	
	Mixed case	
	Excessive use of whitespace	
	Comment removal (e.g. convert DELETE/**/FROM to DELETE FROM)	
	Conversion of (Windows-supported) backslash characters into forward slash characters.	
	Conversion of IIS-specific Unicode encoding (%uXXYY)	
	Decode HTML entities (e.g. c, ", ^)	
	Escaped characters (e.g. \t, \001, \xAA, \uAABB)	

23	The proposed solution should support different policies for different application sections	
24	The proposed solution learning mode should be able to recognize application changes as and when they are conducted while simultaneously protecting web applications	
25	The proposed solution should have the ability to perform behavioral learning to examine traffic and highlight anomalies and provide recommendations that can be turned into actions such as apply, change and apply, ignore etc.	
26	The proposed solution should support line speed throughput and sub-millisecond latency so as not to impact Web application performance.	
27	For SSL-enabled Web applications, the certificates and private/public key pairs for the Web servers being protected need to be up loadable to the Web application firewall.	
28	The proposed solution should have "anti automation" protection which can block the automated attacks that use hacking tools, scripts, frame work etc.	
29	The proposed solution should have an out-of band management port.	
30	The proposed solution should support web based centralized management and reporting for multiple appliances.	
32	The following report formats are deemed of relevance: Word, RTF, HTML, PDF, XML, etc.	
33	Unique transaction ID should be assigned to every HTTP transaction (a transaction being a request and response pair) and included with every log message.	
34	Access logs can periodically be uploaded to the logging server (e.g. via FTP, SFTP, WebDAV, or SCP).	
35	The proposed solution should provide notifications through Email, Syslog, SNMP Trap, Notification via HTTP(S) push etc.	
36	The proposed solution should be able to log full session data once a suspicious transaction is detected.	
37	The proposed solution should provide the admin to manually accept false positives	
38	The proposed solution should be able to recognize trusted hosts	
39	The proposed solution in passive mode should be able to provide impact of rule changes as if they were actively enforced	
40	The proposed solution should support clustered deployment of multiple WAFs sharing the same policy.	
41	The proposed solution should support minimum 5 virtual instances (Environment) from day-1.	
42	The proposed solution should support all operating systems and their versions including but not limited to Windows, AIX, Unix, Linux	

43	The proposed solution should be able to restrict traffic from blacklisted/potentially dangerous sources such as phishing urls, known botnets, malicious Ips etc. Through the use of reputation services.	
44	The proposed solution should provide a high-level dashboard of system status and Web activity.	
45	The proposed solution should be able to generate custom or pre-defined graphical reports on demand or scheduled.	
46	The proposed solution should be able to integrate with the proposed SIEM solution.	
47	Each appliance should have minimum 500 GB Hard disk storage and 1Gbps of WAF throughput from day 1. It should have required number of ports from day 1.	
48	The proposed solution should be able to generate comprehensive event reports with filters:	
	a. Date or time ranges	
	b. IP address ranges	
	c. Types of incidents	
	d. Geo Location of attack source	
	d. Other (please specify).	

6.2.3 VSCDL Requirement for Additional Licenses of Antivirus

VSCDL has a centralized AV Console/Policy and all Servers and Desktops are managed through the following AV solutions. The bidder for this RFP has to supply additional licenses of the following Antivirus product which are centrally deployed at Smart DC of VSCDL.

#	Name	Existing Product
1.	Antivirus for Server	TrendMicro DeepSecurity
2.	Antivirus for Desktop	TrendMicro Officescan XG

6.2.4 HIPS

S No.	Technical Requirement	Compliance (Y/N)
1.	The servers in DMZ, MZ, Management and Public zones should be enabled with Host Based Intrusion Detection & Prevention mechanisms.	
2.	The HIPS should protect against common classes of attacks, including port scans, buffer overflows, Trojan horses, malformed packets, malicious HTML requests, and e-mail worms, etc.	
3.	HIPS should provide automated, real-time intrusion detection and should protect by analyzing the events, operating system logs and inbound/outbound network traffic on enterprise servers.	

4.	The proposed solution should employ full, seven-layer, state-based protocol decoding and analysis. Analyze all packets to and from the server for propagation. To detect and prevent attacks, both known and unknown intrusion attempts. Solution may support prevention of the attacks including but not limited to following: a) Prevents the delivery and installation of kernel-level Root kits. b) Prevents cross-site scripting (XSS) attacks c) Prevents SQL injection attacks d) Prevents DOS, DDOS, worm, botnet and Trojan attacks e) Prevent Buffer overflow attacks f) Decodes backdoor communications and protocols g) Inspect and block attacks that happen over SSL (HTTP & HTTPS).	
5.	The HIPS should use the HTTPS and TLS protocols for the management interface and for the communication between the HIPS and management center. The HIPS should reside between the applications and the kernel, enabling maximum application visibility with minimal impact to the stability and performance of the underlying operating system.	
6.	When an application attempts an operation, the HIPS should check the operation against the application's security policy, making a real-time allow or deny decision on its continuation and determine if logging the request is appropriate.	
7.	By combining security policies implementing distributed firewall, operating system lockdown and integrity assurance, and audit event collection capabilities, the HIPS should provide comprehensive protection for exposed systems.	
8.	It should support Signature as well as behavioral based detection.	
9.	It should support custom policies creation based on user defined inputs	
10.	It should support desktop firewall capabilities to directly block unwanted traffic.	
11.	HIPS solution should provide at least below control detection on Files, Registry, Applications Services – Create Modify Change Permission Read Read/Write Delete	
12.	HIPS Solution should block execution of unwanted applications.	

13.	The offered product series or its operating system series may have achieved EAL (Evaluation Assurance Level) Certification of EAL2 or higher in the Common Criteria.	
14.	The proposed solution may be capable of filtering HTTP requests to prevent directory traversal and denial-of-service (DoS) attacks.	
15.	The proposed solution should provide Executable matching for applications based on path, hash, digital signature and file description for signatures and exception and not just on path basis.	
16.	The proposed solution should be capable of blocking and detecting of IPv6 attacks.	
17.	The proposed solution should have the capability to notify an administrator if any particular log is collected more than a predefined number of times in a set time interval. These alerts should show up on Central Administration console and should be E Mailed to the Administrator. The solution should have capability to forward these events to a SNMP manager & SIEM solution	

6.2.5 Data Loss Protection (DLP)

S. No	Technical Requirement	Compliance (Y/N)
1	The DLP solution should be dedicated on premise solution and should not be part of any other devices asked in the BoQ of this corrigendum	
2	The proposed solution should be able to block/alert pdf content access /Cut/Copy by image writer, or by application like screen capturing /session recording tools etc.	
3	The proposed solution should have wide range of out of the box rule sets	
4	The proposed solution should support the following for rules creation and updation a. centralized console for rule creation and updation b. Ability to whitelist legitimate data format c. Ability to create custom ruleset and apply it on select IP addresses/email IDs / directory groups etc.	
5	The proposed solution should also capture violations made by users to defined policies	
6	The proposed solution should support centralized key management	
7	The proposed Solution should make sure that the agent deployed should not be removed via unauthorized methods or from unauthorized service stoppage.	
8	The proposed solution should provide SSL decryption and destination awareness capability on the gateway to identify any sensitive content uploading to online web properties, even when it is tunnel over SSL	

RFP for Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL
(Second Attempt)

9	The solution should have pre-defined applications and application groups and allow each application/application group to monitor operations like Cut/Copy, Paste, File Access and Screen Capture and also can add the custom applications.	
10	The proposed solution must have the mechanism to index and retain all documents by monitoring all traffic policy rules.	
11	The proposed solution should be able to perform following searches: a. e-mail sent from or to any email address b. traffic sent across protocols or ports c. Documents leaving the network based on document type	
12	The proposed solution should support: a. Scanning file formats such as (Word, excel, ppt, xls) b. Non textual pds, xps c. data in archival tools (.zip/rar/.7z/.tar). Alert presence of encrypted archived files d. analyze encrypted data over web proxies e. analyze data sent over email (organizational/non organizational - Gmail etc), mobile devices.	
13	The proposed solution should be able to monitor IM Traffic even if it is tunneled over HTTP protocol, and FTP traffic including fully correlating transferred file data with control information	
14	The proposed solution should be able to monitor data copied to network file shares and should enforce structured and unstructured fingerprint policies even when disconnected from corporate network.	
15	The proposed solution should create an incident in the central management server or ticketing tool for all critical or high-level impacts	
16	The proposed solution should be able to discover and identity sensitive information stored on endpoints, databases, file shares, SharePoint, SAN, NAS etc.	
17	The proposed solution should have a mechanism to highlight any deviation from policies for storage of sensitive information	
18	The proposed solution should be able to deploy both pattern matching and document tagging with 3rd party and fingerprinting	
19	The proposed solution should be able to schedule periodically recurring scans to identify sensitive data at rest	
20	The proposed solution should have the capability to encrypt the sensitive content when copied.	
21	The proposed solution should Encrypt data transferred to portable media with encryption of 128 bit and above	
22	The proposed solution should be able to monitor movement of sensitive data at endpoint through various channels such as bus, Bluetooth, LPT etc.	

RFP for Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL
(Second Attempt)

23	The proposed solution should be able to inspect documents embedded in other documents	
24	The proposed solution should be able to track the copying of data into USB drives, media cards and mobile phones if they considered as removable media.	
25	The proposed Solution should notify the end user of a policy violation using a customizable pop-up message and should capture content that violates a policy and store it in an evidence repository	
26	The proposed solution should restrict access to sensitive data based on user roles.	
27	The proposed solution should restrict sensitive information from being printed	
28	The proposed Solution should be able to enforce policies for virtual desktops or thin clients	
29	The proposed solution should be able to configure policies to detect on fingerprints and files from share/repository/date created etc.	
30	The proposed solution should enforce policies to detect low and slow data leaks.	
31	The proposed solution should be able to enforce policies to detect data leaks	
32	The proposed solution should have a dashboard view.	
33	The proposed solution should support reports in different formats such as PDF, Excel or CSV format.	
34	The proposed solution should support the following type of analysis Regular expression/pattern matching/indexing/tags Based on file names Full text/ URL requested Should have the capability to check with full/partial documents Should be able to provide information on how many times a user has violated DLP policies	
35	The proposed solution should support the following for analysis Capture the metadata for further inspection Capture SMTP headers, from and destination IP addresses, date/time	
36	The proposed solution should provide an ability to perform full scans and incremental scans	
37	The endpoint agent should be compatible with: Windows OS (32/64 bit) and MAC OS	
38	The proposed solution should have options to see summary reports, trend reports and high-level metrics etc.	
39	The proposed solution should have a mechanism for incidents to be sorted by severity level, sender, recipient, source, destination, protocol and content type	
40	The proposed solution in case of policy violation should be able to detect and alert in real time basis.	
41	The proposed solution should support quarantine capability with escalation review mechanism	
42	The incident should include a clear indication of how the transmission or file violated policy (not just which policy was violated), including clear identification	

	of which content triggered the match and should allow opening of original attachment directly from the UI	
43	The proposed solution should trigger only one incident per event, even if the event violates multiple policies.	
44	The proposed solution should have a mechanism to support easily downloadable upgrades from OEM official website	
45	The proposed solution should be able to integrate with the proposed SIEM solution.	

6.2.6 SIEM

SL. No.	Requirement	Compliance (Y/N)
46	The proposed solution should be on-premise purpose-built appliance(s) comprising of following modules/ functions <ul style="list-style-type: none"> • collection module • logging module correlation module 	
47	The SIEM solution should be supplied with Enterprise wide License and should support project landscape as defined in RFP, Licenses should be calculated appropriately	
48	The proposed solution should support log collection, correlation and alerts for the number of devices /applications mentioned in scope of work.	
49	The proposed solution should be able to support automatic updates of configuration information with minimal user intervention. i.e. security updates, vendor rule updates, device integration support, etc.	
50	The proposed solution must ensure all the system components continue to operate when any other part of the system fails or loses connectivity.	
51	The proposed solution must have an automated backup/recovery process.	
52	The proposed solution must automate internal health checks and notify the user in case of problems.	
53	The proposed solution should be able to perform single site & multi-site correlation across the network.	
54	The proposed solution should provide collection of events through customization of connectors or similar integration for the assets that are not natively supported. They should adhere to industry standards for event collection: syslog, OPSEC, WMI, SDEE, ODBC/JDBC , FTP, SCP, HTTP, text file, CSV, XML file etc	
55	The proposed solutions should be able to collect data from new devices added into the environment, without any disruption to the ongoing data collection.	

56	The proposed solution should have connectors to support all the devices/applications of all project landscape described in this RFP.	
57	In the proposed solution, all logs should be Authenticated (time-stamped across multiple time zones) encrypted and compressed before transmission.	
58	The proposed solution should be able to continue to collect log data during database backup, de-fragmentation and other management scenarios, without any disruption to service	
59	The proposed solution should provide options to load balance incoming logs to multiple collector instances.	
60	The proposed solution should support log collection from all operating systems and their versions including but not limited to Windows, Unix, Linux, etc.	
61	The proposed solution should be able to store/retain both the log meta data and the original raw message of the event log for forensic purposes.	
62	In case the connectivity with SIEM management system is lost, the collector should be able to store the data in its own repository. The retention, deletion, synchronization with SIEM database should be automatic/Manual..	
63	The proposed solution shall allow bandwidth management, rate limiting, at the log collector level.	
64	The proposed solution should ensure that the overall load on the network bandwidth at DC, WAN level is minimal	
65	The proposed solution should provide time based, criticality based store and forward feature at each log collection point	
66	The proposed solution should have the capability to compress the logs by at least 70 % for storage optimization.	
67	The proposed solution should be possible to store the event data in its original format in the central log storage	
68	The data archival should be configured to store information in tamper proof format and should comply with all the relevant regulations.	
69	Traceability of logs shall be maintained from the date of generation to the date of purging.	
70	The proposed solution must support log archives on 3rd party storage.	
71	The proposed system shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.	
72	The proposed solution should be feasible to extract raw logs from the SIEM and transfer to other systems as and when required.	
73	The proposed solution should support the following log collection protocols: Syslog over UDP / TCP, Syslog NG, SDEE, SNMP Version 2 & 3, ODBC/JDBC , FTP, Windows Event Logging Protocol, Opsec, Netflow at a minimum.	

74	The proposed solution should provide mechanism that guarantee delivery of events to the log management system and that no events will get lost if log management system is unavailable	
75	The proposed solution should prevent tampering of any type of logs and log any attempts to tamper logs. It must provide encrypted transmission of log data to the log management.	
76	The proposed solution should allow the creation of an unlimited number of new correlation rules	
77	The proposed solution should be able to integrate with security and threat intelligence feeds data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.) for the purpose of correlating events. These data feeds should be updated automatically by the proposed solution.	
78	The proposed solution should be able to perform the following correlations (but not limited to): Rule based, Vulnerability based, Statistical based, Historical based, Heuristics based, Behavioral based etc. across potentially disparate devices.	
79	The proposed system/solution should have the ability to correlate all the fields in a log	
80	The proposed solution should be able to parse and correlate multi line logs	
81	The proposed solution should have the ability to gather information on real time threats and zero-day attacks issued by anti-virus or IDS/ IPS vendors or audit logs and add this information as intelligence feed in to the SIEM solution via patches or live feeds	
82	The proposed solution should allow a wizard-based interface for rule creation. The proposed solution should support logical operations and nested rules for creation of complex rules	
83	The central correlation engine database should be updated with real time security intelligence updates from OEM	
84	The dashboard should be in the form of a unified portal that can show correlated alerts/ events from multiple disparate sources such as security devices, network devices, enterprise management systems, servers, applications, databases, etc.	
85	Events should be presented in a manner that is independent of device specific syntax and easy to understand for all users	
86	The dashboard should show the status of all the tools deployed as part of the NOC/SOC, including availability, bandwidth consumed, system resources consumed (including database usage)	
87	It should be possible to categorize events while archiving for example, events for network devices, antivirus, servers etc.	
88	Any failures of the event collection infrastructure must be detected and operations personnel must be notified as per SLA. The device Health	

	monitoring must include the ability to validate that original event sources are still sending events	
89	The proposed solution should generate the following reports (but not restricted to): User activity reports, Configuration change reports, Incident tracking report, Attack source reports etc. In addition, the proposed solution should have a reporting writing tool for development of any ad-hoc reports.	
90	The Dashboard design for the proposed solution should be editable on an ad hoc basis as per the individual user need	
91	The proposed system should display all real time events. The proposed solution should have drill down functionality to view individual events from the dashboard	
92	The proposed solution should allow applying filters and sorting to query results.	
93	The proposed solution should allow creating and saving of ad hoc log queries on archived and retained logs. These queries should be able to use standard syntax such as wildcards and regular expressions.	
94	The proposed solution should allow for qualification of security events and incidents for reporting purpose. The proposed solution should be able to generate periodic reports (weekly, monthly basis) for such qualified security events/ incidents.	
95	The proposed solution should provide summary of log stoppage alerts and automatic suppression of alerts.	
96	The proposed solution should generate e-mail and SMS notifications for all critical/high risk alerts triggered from SIEM	
97	The proposed solution should allow users to initiate and track alert related mitigation action items. The portal should allow reports to be generated on pending mitigation activities	
98	The proposed solution should be able to provide asset details such as Asset owner, location, events & incidents, vulnerabilities and issue mitigation tracking mapped to individual assets/users	
99	The proposed solution should provide knowledge base and best practices for various security vulnerabilities	
100	Dashboard should display asset list and capture details including name, location, owner, value, business unit, IP address, platform details	
101	Dashboard should capture the security status of assets and highlight risk level for each asset. This should be used to capture security status of , status of different business units within the VSCDL, status of key locations etc.	
102	The proposed solution should provide the ability to monitoring and alerting on non-compliance events in real-time and provide necessary reports and dashboards.	

103	Dashboard should support reporting for consolidated relevant compliance across all major standards and regulatory requirements. This includes ISO 27001, RBI regulations, IT ACT, PCI DSS standards etc	
104	Dashboard should support different views relevant for different stake holders including top management, operations team, Information Security Department	
105	It should be possible to export data from dashboard to multiple format	
106	Dashboard views should be customizable as per user rights and access to individual components of the application.	
107	Administrators should be able to view correlated events, packet level event details, real-time raw logs and historical events through the dashboard.	
108	Senior Management should be able to view compliance to SLA for all NOC/SOC operations	
109	The proposed solution should permit setting up geographical maps/images on real time dashboards to identify impacted areas and sources of alerts.	
110	The proposed solution should have the capability to identify frequently used queries and provide means to optimize query response time for such queries	
111	The proposed solution should have the ability to perform free text searches for events, incidents, rules and other parameters.	
112	The proposed system should identify the originating system and user details while capturing event data.	
113	The proposed solution should be possible to automatically create incidents and track their closure	
114	The event should reach the SOC monitoring team within 30 seconds of the log being captured	
115	The proposed solution should have a mechanism to track security incidents across a wide range of relevant attributes (i.e. IP addresses, usernames, MAC address, log source, correlation rules, user defined, etc.).	
116	The proposed solution must provide embedded workflow capabilities that security operations staff can use to guide their work	
117	The proposed solution should have the ability to send notification of correlated events via well-defined methods (i.e., SNMP trap, email, etc.)	
118	The proposed solution should offer a means of escalating alerts between various users of the proposed solution, such that if alerts are not acknowledged in a predetermined timeframe, that alert is escalated to ensure it is investigated.	
119	The vendor should provide for adequate storage to meet the EPS and retention requirements of the VSCDL. SI shall be responsible for upgrade of the storage to meet the VSCDL's requirements as above at no additional cost. The SI should provide adequate justification for the storage size proposed as part of the response.	
120	The proposed solution should be able to store both normalized and RAW logs	

121	The platform should provide tiered storage for the online, archival, and backup and restoration of event log information.	
122	The Tier I and II storage should have the capability to authenticate logs on the basis of time, integrity and Origin	
123	The storage solution should have the capability to encrypt/hash the logs in storage	
124	The proposed system should have capacity to maintain the logs for 90 days on Tier I storage and older logs should be archived on Tier II storage and Tier 3 storage	
125	The proposed solution should be capable of retrieving the archived logs for analysis, correlation and reporting purpose automatically.	
126	The proposed solution should be able to part and filter logs before storage on the basis of type of logs; date etc	
127	The proposed solution should be capable to replicate logs in Synchronous as well as Asynchronous mode.	
128	The proposed solution should be possible to define purging and retention rules for log storage.	
129	The proposed solution should come with built-in functionality for archiving data.	
130	The proposed solution should be able to provide specific (Important) DAM reports	
131	The proposed solution should be able to Integrate with IPS, IDS, Firewall, Proxy etc. to identify network security issues	
132	The proposed solution should be able to Integrate with DLP solutions to identify misuse of sensitive information	
133	The proposed solution should be able to Integrate with PIM and other Directory solution to relate security events to user activities	
134	The proposed solution should be able to Integrate with Vulnerability Assessment tools to identify security events	
135	The proposed solution should be able to integrate with GRC solution in future to capture compliance against security policies	
136	The proposed solution should be able to integrate with physical access control systems.	
137	The proposed solution should be able to Integrate with helpdesk/ incident management tools	
138	The proposed solution Should be able to integrate with VSCDL's backup solution for performing backup of the SIEM.	
139	Connector Development tool/SDK availability for developing collection mechanism for home-grown or any other unsupported applications	

140	The proposed solution should provide bi-directional integration with 3rd party trouble ticketing/help desk systems that security operations staff of VSCDL may use.	
141	The proposed system should have out of the box rules for listed IDS/IPS, firewalls routers, switches, VPN devices, antivirus, operating systems, Databases and standard applications etc.	
142	The SI should prepare a DR plan for switch over in case the DC operations are down	
143	The proposed solution should have high availability feature. There should be an automated switch over to secondary collector in case of failure on the primary collector. No performance degradation is permissible even in case of collector failure.	
144	The proposed storage solution should have adequate redundancy for handling disk failures	
145	The proposed Solution should support integration with big data storage configuration such as Hadoop etc	
146	The proposed solution should support creation of automated incident management workflows to track incident from creation to closure, provide reports on pending incidents. It should also permit upload of related evidences such as screenshots etc.	
147	The proposed system should receive feeds from a threat intelligence repository maintained by the OEM which consists of inputs from various threat sources and security devices across the globe.	
148	The Vendor must provide comprehensive support offering, including Phone Support, Email Support, Online community portal to access patches, upgrades new devices support and via online download	
149	The proposed solution should be preferably appliance based solution	

6.2.7 Anti - Advanced Persistent Threat (Anti-APT)

S. No	Technical Requirement	Compliance (Y/N)
1	The solution should be able to inspect and block all network sessions over web protocols for suspicious activities or files at various entry/exit sources to the network.	
2	The solution should be able to protect against Advanced Malware, zero-day web exploits and targeted threats without relying on signature database.	
3	The solution should be able to identify malware present in the following file types and should be able to notify and block across in the relevant stages: Archives: ZIP/RAR/7ZIP/TNEF, jar, Media: MP3, 3GP, ASF, swf, mov, qt,	

	Document: doc, docx, pdf, ppt, pptx, pps, ppsx, rtf, xls, xlsx, Image: jpeg, jpg, jip, gif, png, tiff, Web Objects: com, exe, htm, url, vbs, vcf, chm, dll, ico	
4	The solution should be able to block malware downloads over different protocols.	
5	The solution should be able to identify spear phishing email containing malicious URLs and attachments that bypass the anti-spam technologies.	
6	The solution should support Sandbox test environment which can analyse threats to various operating systems, browsers, desktop applications and plug-ins etc.	
7	The solution should support both inline (via sensors integration) and out of the band mode.	
8	The solution should be able to detect and prevent bot outbreaks (via multiple channels like SMTP, HTTP, HTTPS etc.) including identification of infected machines	
9	The solution should be appliance based with hardened OS. No information should be sent to third party system for analysis of malware automatically.	
10	The solution should be able to block the call back tunnel including fast flux connections. (This feature can be offered as part of NGFW or other equipment of the cyber stack offered)	
11	The solution should be able to integrate with deployed appliances to share malware information/ zero-day attacks knowledge base.	
12	The solution should be able to pinpoint the origin of attack both inside the network (infected machine inside the network) and outside the network (attempted attach from a remote server).	
13	In case there is no antivirus signature available for malware, solution should have the ability to exfiltrate data about the malware and share it with the antivirus solution providers.	
14	The Anti-APT solution should integrate bi-directionally with proposed SIEM to provide alerting and historic views for security intelligence, risk prioritization, and real-time situational awareness.	
15	Dashboard should have the feature to report Malware type, file type, CVE ID, Severity level, time of attack, source and target IPs, IP protocol, attacked ports, Source hosts etc.	
16	The solution should generate periodic reports on attacked ports, malware types, types of vulnerabilities exploited etc.	
17	Solution should be able to monitor encrypted traffic	
18	The management console should be able to provide information about the health of the appliance such as CPU usage, traffic flow etc.	
19	The solution should display the geo-location of the remote command and control server.	
20	The solution should be able to integrate with Active Directory to enforce user-based policies.	

6.2.8 Network Access Control (NAC)

S.No	Technical Requirement	Compliance (Y/N)
1	The solution should support continuous detection of devices attempting to connect to the network	
2	The solution should gather the following data before an endpoint has access to network: Device type,	
	Operating system,	
	User identity,	
	Operating system,	
	Patch status,	
	Anti-virus status,	
	Host firewall status,	
	Known/Unknown device status,	
	Past policy compliance and threat history,	
	Wired/Wireless connection,	
	Windows registry settings,	
3	The solution should have a registration process for the external devices to access internal network and maintain guest access.	
4	The solution should support quarantine mechanism performed both at Layer 2 and Layer 3	
5	The solution should detect handheld devices with platforms such as iPhone/iPad, Android etc.	
6	The solution should detect devices without IP addresses, such as stealthy packet capture devices designed to steal sensitive data.	
7	The solution should be able to integrate with directory services/ identity and access management system for Role-based access facility.	
8	The solution should be able to report violations based on VSCDL's defined device baseline to the SIEM. For example, all endpoints should be in compliance with VSCDL's antivirus policy, should be properly patched and free of unauthorized software etc.	
9	The solution should support standard-based authentication and directories such as 802.1x, Directory services, AAA mechanisms etc.	
10	The solution should be able to link to databases for developing policies. OR	
	The solution should be able to import device list using CSV or integration with MDM solution.	
	For example, retrieve a list of MAC addresses of iPads that are owned by the company, and then a policy can be created to block other iPads	

11	The solution should support third party hardware/software such as Network switches, Wireless Access Points, VPN, Antivirus, Patch Management, Ticketing, SIEM, Vulnerability assessment scanners and MDM.	
12	The solution should support out-of-band deployment.	
13	The solution should support the following mechanisms for access control and policy validation: VLAN Steering, DHCP, Agent based enforcement, Mac Authentication etc	
14	The solution should capture audit logs that contain the following user name , IP, roles , groups, resources accessed, compliance status of endpoint etc.	
15	The solution should be able to detect through periodic monitoring if endpoint security configurations are modified after obtaining access to the network and identify users who have violated in the past.	
16	The solution should support alerting mechanism such as e-mail, SMS etc.	
17	The solution should be able to control access to network as per time, location of user, mode of access, type of system used to access etc.	
18	The solution should be able to detect endpoint Mac address, IP addresses, network resources devices, resources such as printers and scanners, network zones etc. through auto discovery.	
19	The solution should be able to identify and authenticate VPN users	
20	The solution should be able to support virtualized environments.	
21	The solution should integrate with service desk tools to support automated workflow for providing access , change management and exception control	
22	The solution should permit admin to define thresholds for threat levels received from the NAC	
23	The solution should be able detect and manage hand held devices used for financial inclusion process	
24	The Solution should be easily scalable to large number of users.	
25	The Solution should be able to integrate with the proposed SIEM solution.	

6.2.9 Integration / Repositioning of Existing HSM

The bidder is required to integrate existing HSM solution (Which is procured as part of ERP project) into overall cyber security architecture.

6.3 VAPT Information and Remediation Services

VSCDL intends to have Vulnerability Assessment as a service for its critical devices installed at DC & DR and perform Penetration Testing for servers hosted over Internet. The bidder shall carry out Vulnerability Assessment and Penetration Testing activity during implementation phase as well as yearly VAPT activity once every year during O&M period

- a) Bidder should provide vulnerability assessment services for mentioned devices/servers.

- b) Bidder should perform penetration testing for servers hosted over Internet
- c) Bidder should provide detailed reports of the assessment
- d) Bidder should execute this service on Yearly basis

The vendor should carry out Vulnerability Assessment and Penetration testing both internal and external using required software/technical tools for assessing VSCDL's network **on Yearly basis**. The Bidder is to bring his own VAPT tools for testing purpose and obtain required approval for conducting the same. The bidder should provide advisory-cum-remediation services for the Vulnerabilities/Risks detected. The broad scope of work is given below.

- i. The provider shall conduct a detailed study of the existing vulnerability reports and also conduct internal VAPT tests, understanding the background IT infrastructure in the VSCDL.
- ii. Provide steps for fixing the vulnerabilities and/or suggest VSCDL's team of compensating controls that needs to be implemented in order to remediate /circumvent the vulnerability.
- iii. Upon getting VSCDL team's concurrence, proceed with production resolution.
- iv. In the case of application dependencies, the details shall be provided and compensating controls suggested, wherever possible.

6.4 Security/Threat Intelligence Services

VSCDL intends to have a system for tracking of new and emerging threats & vulnerabilities affecting organization across the world so that VSCDL can proactively protect against them.

Bidder should track and provide information on global security threats and help the VSCDL to mitigate the relevant risks on continuous and proactive basis.

The service will include:-

- a) 24*7*365 - Continuous tracking of global threats and vulnerabilities to tackle evolving threats and vulnerabilities.
- b) Provide trusted detailed reports on newly discovered malicious threats and malware in the wild.
- c) Detail the threat with the information appropriate to the VSCDL such as:
 - i. The threat type
 - ii. Risk involved
 - iii. Systems affected
- d) Technical description of the threat and exploit parameters.
- e) Mitigation strategies and the recommendations for the VSCDL to prevent the threat from causing harm to the environment.
- f) Infiltration of malicious hackers and other communities.
- g) Monitoring of network activities and discern risks to the VSCDL environment.
- h) Advisories to the VSCDL on relevant threats and vulnerabilities.

- i) The intelligence content should be able to look at the goals of the threat actor, variants of the threat, current activities implicating the threat, the outcomes for the VSCDL if the threat is successful as well as provide defence against the threat.
- j) Track mitigation against identified risk exposure.
- k) Assists the VSCDL to ensure such threats and vulnerabilities are mitigated in the VSCDL's systems and Provide from the short term plans to the very long term strategies.
- l) Assist the VSCDL in taking relevant decisions Assessment of inherent and residual risk, preferably expressed as impact on business processes, rather than the underlying technology.
- m) The intelligence content should focus more on technical attacks against infrastructure.
- n) The bidder shall be able to provide Integrated Threat Intelligence Feeds from partners and communities (acceptable to the VSCDL) as well as from IB-CART, NCIIPC, CERT-IN, NPCI etc. and shall be able to take advantage of this knowledge to address the threat, preferably using automated tooling standard format such as STIX. The threat intelligence subscription can be included in the O&M cost

6.5 Hardware, Software and Network Connectivity

- a) The bidder needs to provide all the hardware and software required as part of this RFP.
- b) The sizing of the infrastructure as proposed by the bidder, should be certified by the OEM.
- c) The bidder shall ensure that the hardware proposed does not reach end of life (EOL) and end of support (EOS) during the contract period of **Five** years plus addition of two year post completion of the contract.
- d) None of the tools/software/utilities/solutions proposed should be Open Source. Any bid submitted with Open Source tools/software/utilities/solutions will be rejected. Only the IT assessment tool needs to be open source.
- e) The bidder will be given the rack space at DC and connectivity between DC and DR by the VSCDL, all other necessary hardware and peripherals are to be provided by the bidder. Details of such hardware needs to be given in the Bid.
- f) Bidder should consider sizing as per project details given in **section 1.15** of this corrigendum and integration of additional **endpoints/ switches/ network devices** during the contract period considering minimum 5% growth every year. VSCDL will not be responsible to pay for any additional cost other than the cost mentioned in commercial bid.
- g) The network connectivity between VSCDL offices, Data Centre site and Disaster Recovery Site will be provided by the VSCDL. The bidder will be responsible for any other network connectivity required for CSOC operations.

6.6 Training

Deployment of VSCDL staff for CSOC operations

In addition to existing IT staff, VSCDL is desire of recruiting own staff/interns for supporting operations of CSOC. These staff will receive above training. Such staff would be deployed by VSCDL as L1 and L2 CSOC operational staff to assist CSOC operations. SI should impart training to all such staff.

The aim is to make this CSOC as centre of excellence in smart city cyber security operations and emerges as role model for other smart cities.

Considering above scenario the training to VSCDL staff becomes very much important. The training plan for VSCDL personnel/SOC team is modified as per the table provided below:

	Solution	Training Time	
		Pre-Implementation (Days)	Post-Implementation (Days)
	Phase I		
1	NG Firewall (External) (1+1 in HA mode)	1	1
2	Web Application Firewall solution	1	2
3	SIEM solution	1	2
4	PIM Solution	1	2
	Phase II		
5	Server Security (HIPS) (For servers)	1	1
6	DLP Solution (End point, Web, Network, File Share)	1	2
7	Anti APT Solution	1	2
8	NAC (Network Access Control) Solution	1	1
9	2 Factor Authentication	1	1

- Pre-Implementation:** Provide training to the VSCDL personnel/ SOC team on the product architecture, functionality and the design for each solution under the scope of this RFP.
- Post Implementation:** Provide hands-on training to the VSCDL personnel/ SOC team on SIEM operations, alert monitoring, policy configuration for all solutions etc.
- The bidder and OEM are required to provide training jointly as per the below table for people nominated by the VSCDL for each solution specified in the scope of work.
- The bidder and OEM are required to provide ad-hoc trainings to the VSCDL staff, to acquaint them with the latest features and functionalities of the solutions for minimum of one day. VSCDL has the right to exercise this training option at its discretion. The cost of this training would need to be quoted in the Commercial Bid by the bidder in the pre-defined field.
- The bidder is required to provide all trainees with detailed training material and 2 additional copies to the VSCDL for each solution as per the scope of work of the VSCDL. This training material should cover installation, operation, integration, maintenance, troubleshooting and other necessary areas for each solution.
- All out of pocket expenses related to training shall be borne by the selected bidder.
- The bidder may utilize the OEM resources in case the bidder does not have adequately experienced resources for providing training.

6.7 Implementation & Integration

The implementation should cover the technical features as mentioned in Annexure 11.1 to 11.6.

- a) Implementation should comply with the policy released by MoHUA, the Government of India, released a model framework for cyber security in smart cities and other relevant policy mentioned in

RFP section 2.6. and other cyber security related policy released by GOI during implementation phase.

- b) The solution, service, hardware, software and storage services would be provided by the bidder. The VSCDL will provide facilities to host the devices and office arrangement for the personnel.
- c) A comprehensive strategy should be provided by the Bidder on implementing the end to end CSOC solution within 7 days of issuance of Purchase Order (PO).
- d) Once the purchase order (PO) is issued, the successful bidder is required to review the VSCDL environment and specify any additional requirements that the VSCDLs may need to provide for the implementation of the solution.
- e) Bidder has to develop the project plan, get it approved by the VSCDL and then implement the project based on timelines agreed.
- f) The bidder is responsible to ensure that the CSOC solutions and operations comply with industry leading standards (such as ISO 27001, ISO 22301, PCI DSS, Privacy Laws and Regulations etc.) and any applicable laws and regulations such as RBI Guidelines during the contract period.
- g) A comprehensive onsite warranty for a period of 5 years and additional AMC cost for 2nd Year onwards shall be there on all the Hardware and Software supplied to/purchased by the VSCDL.
- h) The bidders needs to provide warranty for entire 5 years at the start of contract period and warranty period will commence from the acceptance date of phase-1 GO-LIVE from VSCDL.
- i) In addition, the bidder is responsible for impact assessment and modification of SOC operations at no extra cost, on account of any changes to applicable information security policies/ procedures / standards/ regulations. Bidder should consider sizing as part of integration of additional devices during the contract period. VSCDL will not be responsible to pay for any further hardware cost.
- j) The bidder would be responsible for updates, patches, bug fixes, version upgrades for the entire infrastructure. VSCDL will not be responsible to pay for any additional cost required as part of additional capacity required.
- k) The Bidder should provide the latest version of the Solution. The bidder would be responsible for replacing the out-of-support, out-of-service, end-of-life, undersized, infrastructure elements at no extra cost to the VSCDL during the contract period. Replacement to be done before 15 days from due of date of the product/service.
- l) The support for all the solutions proposed should be provided for the contract period. Whereas free upgrade should be provided for all solutions if the end of life occurs within the period of contract with VSCDL. The Updates/ Upgrades for medium and low should be implemented within *3 days* of release of the same. For critical and high upgrades / updates, implementation to be implemented within *1 day* of release.
- m) All the solutions supplied as part of this RFP should be supplied with Enterprise wide License. The licenses should be perpetual from the first day with no dependence on payment quoted in the commercial bid and VSCDL wants the licenses to continue to be an integral asset of the VSCDL in perpetuity.
- n) Integrate each solution with SIEM solution to provide a single view of events generated.
- o) Bidder is responsible for developing and implementing the security configuration hardening of all the devices and software that are procured for Security Operations centre. Also, they have to periodically review the guidelines and configure as and when required.

- p) Any interfaces required with existing applications/ infrastructure within the VSCDL should be developed by the bidder for successful implementation of the CSOC as per the defined scope of VSCDL.
- q) Bidder shall be responsible for timely compliance of all Device level audit (DLA) and Vulnerability Assessment (VA) audit observations as and when shared by the VSCDL.
- r) In case the CSOC on-going operations are part of scope for a particular VSCDL, the bidder is responsible for integrating any additional logs that the VSCDL may wish to monitor with the SIEM solution at no additional cost to the VSCDL.
- s) The primary responsibility of integration of new solutions with implemented SIEM lies with the Bidder selected through this RFP.
- t) Development and implementation of processes for management and operation of the CSOC including (but not limited to) the following processes:
 - i. Configuration and Change Management
 - ii. Incident and Escalation management processes
 - iii. Daily standard operating procedures
 - iv. Training procedures and material
 - v. Reporting metrics and continuous improvement procedures
 - vi. Data retention and disposal procedures
 - vii. BCP and DR plan and procedures for CSOC
 - viii. Security Patch management procedure
- u) Implement necessary security measures for ensuring the information and cyber security of the proposed CSOC. This should also be in line with RBI Guidelines.
- v) Develop Escalation Matrix in order to handle Information and cyber Security Incidents efficiently.
- w) Provide necessary documentation including Standard Operating Procedures (SOPs), user manuals, SRS document, Design document, Architecture diagram, etc. for the operation, integration, customization, and training of each of the solutions in scope.
- x) The Bidder would be responsible for installation, testing, commissioning, configuring, warranty and maintenance of the system. The bidder will also provide necessary support and coordination for conducting BCP/DR drill and testing as per VSCDL BCM and IT security policy.
- y) In case a device goes down at DC, the operation and function being performed by the device should be taken over by a corresponding device at DR site and vice versa.
- z) OEM would be responsible for all technical support to maintain the required uptime through the Bidder. Initial installation, configuration and integration should be done by the OEM, through the Bidder. The Bidder would be the single point of contact. The Bidder should have necessary agreement with the OEM for all the required onsite support for entire project period. Bidder should have back-to-back support with OEM during the total contract period for necessary support. OEM should review and certify the successful implementation.
- aa) All the tools supplied as part of this RFP should be supplied with Enterprise wide License and the licenses should be perpetual from the first day with no dependence on payment. VSCDL will have the right to use the tools for the functions provided by the tools in any manner and for any number of branches, offices, subsidiary units, joint ventures, irrespective of the number of users, geographical

location of the devices being monitored. VSCDL will also have a right to relocate any one or all the tools to different locations.

- bb) Bidder shall provide list of licenses to be procured, also maintain the inventory database of all the licenses and the updates installed. Also, the licenses should be in the name of VSCDL.
- cc) The period of support coverage would be for the entire contract period.
- dd) Bidder should provide utilization details that can affect the existing IT infrastructure.
- ee) Adherence to agreed Service Level Agreements (SLA) and periodic monitoring and reporting of the same to the VSCDL through a portal.
- ff) The bidder needs to ensure that CSOC solution can integrate with the IT System and applications using standard methods/ protocols/ message formats for capturing logs, alerts and for monitoring purposes. No changes should be proposed to VSCDL in existing applications and system by bidder.
- gg) CSOC setup / infrastructure may be subjected to audit from VSCDL and/or third party and/or regulatory body. It shall be responsibility of the Bidder to co-operate and provide necessary information and support to the auditors. The Bidder must ensure that the audit observations are closed on top priority and to the satisfaction of the VSCDL, regulator and its appointed auditors. Extreme care should be taken by the Bidder to ensure that the observations do not get repeated in subsequent audits. Such non-compliance by Bidder shall attract penalty.
- hh) CSOC set up should assure the compliance to the Indian regulatory requirements, ISO27001 standards and also international regulations and laws where VSCDL has its presence. The bidder is expected to study the regulations and comply with them as and when mandated.

6.8 Reporting

- a) The bidder should provide periodic reports to the VSCDL as per the following requirements:
 - i) Daily Reports: Critical reports should be submitted by 11:00 AM
 - ii) Weekly Reports: By 11:00 AM, Monday
 - iii) Monthly Reports: 3rd working day of each month
- b) The following list captures a few of the reports which will be provided by the selected Bidder once on boarded. The bidder is expected to detail every report which it will provide to the VSCDL related to the services and activities performed by it in the CSOC:
 - i) Solution design documents for each solution designed for the VSCDL's environment
 - ii) Implementation guide for the solutions implemented at the VSCDL's premises
 - iii) Operations guide for all the solutions managed by the Bidder
 - iv) Incident management playbook which will govern the process followed for handling of incidents as per the defined incident types and the severity
 - v) Weekly and monthly incident tracker and statistics capturing detailed information on the incident identified, its severity, the response by the team, the time taken from identification till closure of the incident and other relevant information
 - vi) Periodic reporting and status tracking / capturing the details of the log sources reporting to the SIEM manager
 - vii) Periodic reports capturing the incidents notified by the SIEM solution
 - viii) Periodic reports capturing the malwares detected and / or prevented by the anti-malware solution.

- ix) Periodic reports capturing the phishing attempts detected and / or prevented by the anti-phishing solution.

6.9 System Integration Testing (SIT) and User Acceptance Testing (UAT)

- a) There will be a User Acceptance Testing by the VSCDL for the tools deployed and CSOC operations.
- b) The VSCDL shall commence the User Acceptance Testing as and when each and every solution and services are made ready by the Bidder and a formal confirmation that the system is ready for UAT is submitted to the VSCDL. The results thereafter will be jointly analyzed by all concerned parties.
- c) UAT will cover acceptance testing of all the product/services, integration with CSOC tools (Primarily SIEM) and integration of CSOC with all targeted devices/systems.
- d) The Bidder is expected to make all necessary modifications to CSOC solution including customizations, interfaces, appliances, software etc., if there are performance issues and errors identified by the VSCDL. These deviations/ discrepancies/ errors observed will have to be resolved by the Bidder immediately.
- e) Complete acceptance has to adhere to the stipulated time lines.
- f) The VSCDL will accept the solution on satisfactory completion of the above inspection. The contract tenure for the Solution will commence after acceptance of the solution by the VSCDL.
- g) In case of discrepancy in facilities /services provided, the VSCDL reserves the right to cancel the entire contract.

6.10 Monitoring

The bidder is required to provide the resource count for the operations of the CSOC as per this corrigendum and provide details and CV's as per Annexure **Section 10.7 TQ_5** of RFP. The bidder should monitor CSOC activities and events from each solution and devices already present in the VSCDL's environment on a 8X7X365 basis and suggest/ take appropriate action on an on-going basis

Type	Role
L1	<ul style="list-style-type: none">• Event monitoring & alert/Incident tracking; regular solution administration.• Fine tuning of the false positive events• Categorization of requests into functional clarification and provision of workaround• Bug identification/change requests to be logged and reported for further processing• Provide telephonic and / or electronic mechanisms for problem reporting requests as well as for service and status updates• Preparation of incident reports
L2	<ul style="list-style-type: none">• Provide continuous onsite support for the implementation of CSOC solution and support for integrating any applications to be interfaced with SIEM solution in future.• Troubleshoot at various levels in the CSOC Solution implementation• Resolve the call within stipulated timeframe as defined in Service Level Agreement

	<ul style="list-style-type: none"> • Coordinate with the L1 & L3 team for resolution and provide necessary information as may be required by the team to resolve the issues. Escalate the unresolved calls as per escalation matrix • Provide the timeframe for providing a solution of resolution of the escalated calls and automatically log calls during escalation • Prepare a root cause analysis document with the resolutions provided for major issues such as production issues, service disruptions or downtime, delayed response times, data/ table corruptions, system performance issues (high utilization levels) etc. • Perform the application audit on a quarterly basis or as mutually agreed with the VSCDL and rectify any corruption in the software • Ensure patch releases are ported to the production environment with no business disruption or business losses • Support periodic BCP/DR drills • Routing the events through the backup system in case the primary system fails • Providing VSCDL with daily hardware utilization reports and alerting VSCDL in case of any performance issues or hardware upgradation requirements • Preparation of incident reports and periodic reporting of critical incidents to management team of VSCDL
L3	<ul style="list-style-type: none"> • Resolve the call within the stipulated timeframe as defined under the service level agreements • Communicate the status of the call to the VSCDL and accordingly update the status, resolution or workaround and date of resolution • Prepare a root cause analysis document for issues referred to L3 support and provide to the VSCDL along with the resolution • Liaise with the L2 support personnel for the call information and resolution. • Perform version upgrades/migration as per the version release plan of OEM and agreed by the VSCDL. • Provide training to the VSCDL's team on CSOC solution and new version functionalities

- VSCDL reserves the right to conduct interviews of the proposed team members for CSOC operations.
- Review L3 resource should assist VSCDL in governance of security event monitoring and incident/alert tracking and assist VSCDL to comply compliance with RBI Guidelines and Indian Cyber Regulations.
- L3 resource should be present onsite for monitoring and operational activities and should act as team leader.
- In case of absence of a lower level resource, a higher level resource should perform the job of the absentee but the payment will be made as per the payment structure of lower level resource only.
- If any resource is absent, standby resources should be available. VSCDL may reject such manpower if VSCDL is not satisfied with his/her performance and payment will be made to bidder as per actual manpower support provided subject to adherence to SLA conditions.

- In case of resource replacement, bidder shall ensure proper Knowledge Transfer (KT) / handover is provided to new resource.
- Per Man Day Charges (to accommodate deduction on account of absence) = Charges per Man Year / (12 x No. of working days in a Month).

6.11 Continuous Improvement

- a) Improve the policies configured on an on-going basis to reduce the occurrence of false positives.
- b) Periodic health check should be carried out on-site, by the OEM every year to ensure the quality of implementation and operations.
- c) Bidder shall curtail the closure time for incidents and events, also ensure the periodic check-up reviews for the same.
- d) Bidder needs to update all solutions and Cyber Security Operations Centre (CSOC) based on any new regulations and RBI guidelines

6.12 SLA Compliance

The bidder shall ensure compliance with SLAs as defined in the section 7 of RFP.

6.13 Business continuity

The bidder is responsible for defining a DR/ BCP plan for the CSOC operations and also ensure that periodic tests are conducted as per the testing calendar agreed with the VSCDL.

6.14 Period of Contract

- a) Bidder is required to provide the services for a period of 5 years extendable for a further duration of maximum two years at the discretion of the VSCDL on the same terms and conditions.
- b) Post completion of the contract/ or in the event of early termination, the bidder is expected to provide support for transition of the services to the nominated members of the VSCDL (or) to a third party nominated by the VSCDL for a period of 6 months.
- c) The Bidder is required to provide the warranty / AMC services at VSCDL's DC / DR and other locations for which tools are procured or where tools are deployed, directly or through their OEM representatives at all locations for VSCDL.
- d) The bidders are expected to provide technical and commercial proposals in accordance with the terms and conditions contained herein. Evaluation criteria, evaluation of the responses to the RFP and subsequent selection of the successful bidder shall be as per the process defined in this RFP. Their decision shall be final and no correspondence about the decision shall be entertained.
- e) In case of termination of contract / end of contract period, bidder has to provide extended services, with the rates mentioned as of last year. This extension of services to be provided till procurement of next solution / till 1 year, with same terms and conditions.
- f) If any support is required after the contract w.r.t. to logs, the bidder has to provide the same (This support would be required in extreme cases only).
- g) Bidder shall provide transition support, which amongst other shall include provision of logs, rules, technical architecture of solution as deployed, detailed description of the processes, etc. as part of the

transition to subsequent bidder or VSCDL on completion or on termination of contract. The support will be for a period of 6 months.

6.15 Deployment of CSOC Operations Personnel during O&M Period

Sr.	Level	Minimum Qualification
1	SOC Lead Cybersecurity Governance - CISO	Graduate in engineering with minimum 8 years of IT experience out of which minimum 5 years in information/cyber security advisory & audit which includes minimum of 2 years of experience in Security Operations Center and 1 year of experience as CISO/CSOC Head. In Addition, he/she should have at least one certification out of the following: <ul style="list-style-type: none"> • CISA • CISSP • ISO 27001 LA • CEH /GCIH / CHFI / OSCE / ECSA
2	Enterprise Application Security Professional (L3 level)	Graduated in engineering with minimum 5 years of IT experience including minimum of 3 years of experience as L3 resource in CSOC implementation
3	Data Protection Analysts IoT / Endpoint Security (L2 Level)	Graduated in engineering with minimum 3 years of IT experience including minimum of 1 years of experience as L2 resource in CSOC implementation
4	IT Auditor/ Analysts (L1 Level)	Graduated in engineering with minimum 2 years of IT experience including minimum of 1 years of experience as L1 resource in CSOC implementation

Level	Role
L1	<ul style="list-style-type: none"> • Event monitoring & alert/Incident tracking; regular solution administration. • Fine tuning of the false positive events • Categorization of requests into functional clarification and provision of workaround • Bug identification/change requests to be logged and reported for further processing • Provide telephonic and / or electronic mechanisms for problem reporting requests as well as for service and status updates • Preparation of incident reports
L2	<ul style="list-style-type: none"> • Provide continuous onsite support for the implementation of CSOC solution and support for integrating any applications to be interfaced with SIEM solution in future. • Troubleshoot at various levels in the CSOC Solution implementation • Resolve the call within stipulated timeframe as defined in Service Level Agreement • Coordinate with the L1 & L3 team for resolution and provide necessary information as may be required by the team to resolve the issues. Escalate the unresolved calls as per escalation matrix • Provide the timeframe for providing a solution of resolution of the escalated calls and automatically log calls during escalation

	<ul style="list-style-type: none"> • Prepare a root cause analysis document with the resolutions provided for major issues such as production issues, service disruptions or downtime, delayed response times, data/ table corruptions, system performance issues (high utilization levels) etc. • Perform the application audit on a quarterly basis or as mutually agreed with the VSCDL and rectify any corruption in the software • Ensure patch releases are ported to the production environment with no business disruption or business losses • Support periodic BCP/DR drills • Routing the events through the backup system in case the primary system fails • Providing VSCDL with daily hardware utilization reports and alerting VSCDL in case of any performance issues or hardware upgradation requirements • Preparation of incident reports and periodic reporting of critical incidents to management team of VSCDL
L3	<ul style="list-style-type: none"> • Resolve the call within the stipulated timeframe as defined under the service level agreements • Communicate the status of the call to the VSCDL and accordingly update the status, resolution or workaround and date of resolution • Prepare a root cause analysis document for issues referred to L3 support and provide to the VSCDL along with the resolution • Liaise with the L2 support personnel for the call information and resolution. • Perform version upgrades/migration as per the version release plan of OEM and agreed by the VSCDL. • Provide training to the VSCDL's team on CSOC solution and new version functionalities

7 Project Phases, Work Completion Timelines & Payment Terms

7.1 Project phases

The project shall be executed in two phases

#	Phase of the Project	Phase Description	To be ordered on
1	Phase I	Solution/Equipment Defined in Phase I: Essential and Critical Cyber Security Equipment needed to kick-start the project within available funds. Manpower : Basic team of CSOC, headed by CISO and L1, L2, L3 Personnel. Will operate only in one shift.	Request Order 1 will be issued immediately after LoI for the project to the successful bidder
2	Phase II	Solution/Equipment Defined in Phase II: Additional Cyber Security Equipment needed to run full-blown CSOC along with all remaining cyber solutions.	Request Order 2 will be issued to the successful bidder, depending upon availability of the funds, within 1 year of Request Order 1 date.

Phase I & II equipment list is given in Section 5.1.1 (Scope of Work)

7.2 Request Orders –

As indicated above, there will be multiple Request orders.

VSCDL shall issue a “Work Orders” in writing, indicating the number of units of Hardware and Software to be supplied along with the location (Project Site).. Upon getting the Work Order, the implementation vendor shall promptly and as soon as possible within the timelines specified in the Work order, supply, install/implement, configure, test, commission and make go-live s hardware and software at stated project site. VSCDL’s decision in this regard shall be. Delay or non–performance will form the basis for application of Liquidated Damages.

7.3 Further milestones and payment schedules

Revised Project Milestones and Payment Schedules for Implementation

Phase I (T1 = Date of Request Order 1)

#	Milestone Description	Timelines to complete	Payment Amount
1.	Inception report including outline of Cyber security and requirements, Project Plan, Reporting Formats, work plan, documentation formats, dates and Submission of Proof of Placement of orders to all OEM, for the requires solution hardware and software in Phase I	T1+1 month	2% of Schedule A
2.	Submission and Acceptance of the following documents <ul style="list-style-type: none"> Draft Cyber security and IT audit report, 	T1+2 month	3% of Schedule A

#	Milestone Description	Timelines to complete	Payment Amount
	<ul style="list-style-type: none"> Information Security related Policies and Guidelines, Cyber Crisis Management Plan (CCMP) for VSCDL IT Facilities which will contain strategy followed in case of a Cyber-attack or threat in VSCDL. Risk Mitigation Report for Cyber Security Policies 		
3.	Presentations on the above documents/policies, its findings, conclusions, and recommendations for Gap Analysis and Plugging, need to be made to the management of VSCDL as required.	T1+3 month	5% of Schedule A
4.	Successful delivery and acceptance of the Hardware/Software for individual Cyber Security solution, after post-delivery audit, on submission of invoice with Proof of Delivery and other documents	T1+3 months	55% of Schedule A
5.	Successful Installation, Configuration and Commissioning of CSOC, along with SIEM and all other Cyber Security Solution components	T1+5 months	5% of Schedule A + 30% of Schedule B
6.	Integration of SIEM with other all other Security Tools / Solutions under CSOC	T1+6 months	5% of Schedule A + 30% of Schedule B
7.	User Acceptance Testing and making CSOC operational	T1+7 months	5% of Schedule A + 20% of Schedule B
8.	Go-live of the CSOC and All Cyber security Solutions	T1+8 months	10% of Schedule A + 10% of Schedule B

Phase II (T2 = Date of Request Order 2)

#	Milestone Description	Timelines to complete	Payment Amount
1	Submission of Proof of Placement of orders to all OEM, for the required Phase II solution hardware and software	T2+15 Days	NA
2.	Successful delivery and acceptance of the Hardware/Software for individual Cyber Security solution, after post-delivery audit, on submission of invoice with Proof of Delivery and other documents	T2+3 months	65% of Schedule E
3.	Successful Installation, Configuration and Commissioning of CSOC, along with SIEM and all other Cyber Security Solution components	T2+ 3.5 months	5% of Schedule E + 30% of Schedule F
4.	Integration of Phase II equipment/ Solution with SIEM and Phase I Security Tools / Solutions.	T2+4 months	5% of Schedule E + 30% of Schedule F

#	Milestone Description	Timelines to complete	Payment Amount
5.	User Acceptance Testing for Phase II equipment/ Solution and making them operational in CSOC	T2+4.5 months	5% of Schedule E + 20% of Schedule F
6.	Go-live of Phase II equipment/ Solution and Go Live of entire project	T2+5 months	10% of Schedule E + 10% of Schedule F

Terms and Conditions Phase I & II:

- The payment timelines will be adjusted based on the adherence to performance of the successful bidder as per implementation timeline.
- The remaining 10% of payment for each phase will be given as equal quarterly payments over a period of 1-year post Go-Live of that phase i.e. 2.5% at the end of every quarter for 4 quarters (2.5% x 4 = 10%).**
- All payments to the Implementation Vendor shall be made upon submission of invoices along with necessary approval certificates from concerned Authority like VSCDL.
- The above payments are subject to meeting of SLA's failing which the appropriate deductions as mentioned in the SLA document of this RFP.

For Operation and Maintenance Period – Phase I & II

#	Phase of the Project	Milestone Description	Payment Amount
1.	O&M	AMC Support Charges	Quarterly payment (at end of the Quarter), after deducting applicable penalties/LD (Schedule C for Phase I & Schedule G for Phase II)
2.	O&M	Manpower Deployment Charges	Quarterly payment (at end of the quarter), after deducting applicable penalties/LD (Schedule D for Phase I)

O&M period will start from the date of Go-live and would be for five years. For example, if the go-live of Phase 1 is from 1st January 2021 then O&M period would be considered from 1st January 2021 to 31st December 2025.

Phase II O&M will also be considered in the similar manner.

Terms and Conditions:

- No payment made by VSCDL herein shall be deemed to constitute acceptance by VSCDL of the system or any subsystem(s).
- VSCDL may withhold 10% of the amount of bill produce by the service provider; for quality check. The cumulative amount will be paid to the service provider at the end of the Project after completion of all contractual obligations, without any interest.
- The Service Provider will submit the Bills as per the terms & conditions of the Bid Document and subject to the successful implementation of IT Audit – Systems Audit and IT Infrastructure Audit at VSCDL.

- ❖ VSCDL will release the payment within 30 days of submission of valid invoice subject to the condition that invoice and all supporting documents produced are in order and work is performed to the satisfaction of VSCDL. After the submission of reports, VSCDL shall take 15 days for review and feedback. VSCDL can extend this duration by 10 days by informing 1 day before the expiry of 15 days interval.
- ❖ Report shall not be considered as submitted without a written concurrence from VSCDL.
- ❖ VSCDL shall be entitled to delay or withhold the payment of any invoice or part of it delivered by Service Provider, when VSCDL disputes such invoice or part of it, provided that such dispute is bonafide.
- ❖ All payments shall be made for the corresponding services delivered as per the Contract Implementation Schedule, at unit prices and in the currencies specified in the Commercial Bids.
- ❖ Any penalties / liquidated damages imposed on the bidder for non-performance will be deducted from the payment as deemed necessary
- ❖ The Selected Bidder shall be responsible for delivery; implementation and rollout of all the solutions required under this RFP and must adhere to the timeline as specified in project timeline in the RFP.
- ❖ In the event of Bidder's failure to deliver and/or implement all required components of a fully functional system (pertaining to the scope of the project) within the stipulated time schedule or by the date extended by the VSCDL, unless such failure is due to reasons entirely attributable to the VSCDL, it will be a breach of contract. In such case, the VSCDL would be entitled to charge a penalty or will have the right to terminate the contract, as specified in this RFP.

8 Service Level Agreement

The purpose of this Service Level Agreement (hereinafter referred to as SLA) is to clearly define the levels of service which shall be provided by the selected vendor to VSCDL for the duration of this contract.

The benefits of this SLA are to:

- Trigger a process that applies VSCDL and the selected vendor management attention to some aspect of performance when that aspect drops below an agreed upon threshold, or target.
- Makes explicit the expectations that VSCDL has for performance.
- Helps VSCDL control the levels and performance of selected vendor services.

The selected vendor and VSCDL shall maintain a regular contact to monitor the performance of the services being provided by the selected vendor and the effectiveness of this SLA. This Service Level Agreement is between the selected vendor and VSCDL.

8.1 Service Level Agreement

Following are the criticality levels of the services to be rendered by the Contractor under this contract. The resolution time shall not exceed the stipulated time for the Metric given in the below table. All the calls are to be closed within specified Service Level Agreement (SLA), irrespective of time the call is registered. The Service Level Agreements (SLAs) covered will be calculated on 24 hours a day 7 days a week basis.

Note: If total penalty amount crosses 10% of overall contract value, VSCDL reserve the right to invoke Annulment of the Contract.

Service Level Agreement

- The purpose of this Service Level Requirements/Agreement (hereinafter referred to as SLR/SLA) is to clearly define the levels of service which shall be provided by the Implementation Agency to the Client for the duration of this contract period of the Project.
- Timelines specified in the above section (**Work Completion Timelines and Payment Terms**) shall form the Service Levels for delivery of Services specified there-in.
- All the payments to the System Integrator (SI) are linked to the compliance with the SLA metrics specified in this document.
- The project Service Level Agreement are proposed to be performance based. For purposes of Service Level Agreement, the definitions and terms as specified along with the following terms shall have the meanings set forth below:
 1. “Uptime” shall mean the time period for which the specified services/components with specified technical and service standards are available for the application. Uptime, in percentage, of any component (Non-IT and IT) can be calculated as:
$$\text{Uptime} = \{1 - [(\text{System Downtime}) / (\text{Total Time} - \text{Planned Maintenance Time})]\} * 100$$
 2. “Downtime” shall mean the time period for which the specified services are not available for the Users, the scheduled outages/planned maintenance time planned in advance for application. The planned maintenance time/scheduled downtime will include activities like software upgrades, patch management, security software installations etc.

3. The selected SI will be required to schedule 'planned maintenance time' with prior approval of Client. This will be planned outside working time. In exceptional circumstances, Client may allow the SI to plan scheduled downtime in the working hours.
 4. "Incident" refers to any event/abnormalities in the functioning of the application, and services that may lead to disruption in normal operations.
 5. "Helpdesk Support" shall mean the 24x7x365 centre which shall handle Fault Reporting, Trouble Ticketing and related enquiries during this contract.
 6. "Response Time" shall mean the time incident is reported to the help desk and an engineer is assigned for the call.
 7. "Resolution Time" shall mean the time taken (after the incident has been reported at the helpdesk), in resolving (diagnosing, troubleshooting and fixing) or escalating (to the second level) getting the confirmatory details about the same from the SI and conveying the same to the end user), the services related troubles during the first level escalation.
- The resolution time shall vary based on the severity of the incident reported at the help desk. The severity would be as follows:
 1. Level 3 (Critical/High): The application is down impacting critical business functions or multiple modules/ functions down impacting users on daily operations or any module/functionality deemed as highly critical by VSCDL.
 2. Level 2 (Medium): One module/functionality down impacting critical business functions having major impact on daily operations.
 3. Level 1 (Low): Loss of business functionality for less than 10 users impacting day to day operations or minor functionality down impacting less than 10 users.

8.1.1 SLA for Project Implementation

The successful bidder will adhere to the project implementation schedule. The Service Level Agreements (SLA) and the applicable penalties in case of non-adherence to project delivery timelines is specified in Relevant Section .

Definition	Timely delivery of deliverables, entire bill of material and as per successful UAT of the same.
Service Level Requirement	All the deliverables defined in the contract has to be submitted on-time on the date as mentioned in the contract with no delay.
Measurement of Service Level Parameter	To be measured in number of weeks of delay from the timelines mentioned in the Section 11 "Work Completion Timelines & Payment Terms".
Penalty for Non-achievement of SLA Requirement	Any delay in the delivery of the project deliverables (solely attributable to vendor) would attract a liquidated damage per week of 0.2% of the CAPEX value of the equipment's/solution delivered (Line Item) per week for first 8 weeks and 0.3% per week for every subsequent week. If the liquidated damage reaches 10% of the total contract value, VSCDL may invoke termination clause. Liquidated damage will be computed on CAPEX value of Contract/Request Order value of the particular phase.

8.1.2 SLA for System Uptime (Solution Uptime)

The bidder has to design the system solution in such way that the system uptime should be 99.5%. The system uptime shall be measured on Monthly basis. In case of system uptime falls below 99.5%, penalty as per following shall be applicable.

The percentage uptime is calculated on a monthly basis (24 hours a day): **(Total contracted minutes in a month - Downtime minutes within contracted minutes in a month) x 100 / Total Contracted Minutes in a Month.**

- VSCDL may recover such amount of penalties due to delay in service from any payment being released to the vendor, irrespective of the fact whether such payment is relating to this contract or otherwise. The same may be recovered from the payment due towards the vendor or from the retention money at the end of contract period.
- The sum total of penalties will not exceed 10% of the Total Cost of Ownership (TCO) within the contract period. Thereafter, the contract/purchase order may be cancelled and performance bank guarantee may be revoked.

The SLAs for System Uptime are modified as per the table given below:

S. No.	Service Area	Uptime % calculated on quarterly basis	Liquidated Damages (LD)
1	CSOC Operations including any device (hardware / software) failure resulting in failure of CSOC operations	99% and above	NA
		98.99% to 97%	1% of Total CSOC Monitoring and Operations cost (Total Opex) for the quarter
		96.99% to 95%	2% of Total CSOC Monitoring and Operations cost (Total Opex) for the quarter
		Less than 95%	3% of Total CSOC Monitoring and Operations cost (Total Opex) for the quarter
2	Individual Security / Device solution (Hardware / Software) Failure. SIEM failure will be considered as total failure and liquidated damage will be as per the point 1.	99% and above	NA
		98.99% to 97%	1% of AMC charges (of that device/solution) for each failure
		96.99% to 95%	3% of AMC charges (of that device/solution) for each failure
		Less than 95%	5% of AMC charges (of that device/solution) for each failure

Terms and Conditions

- For hardware / software items whether under AMC or under warranty, notional AMC / License fee shall be calculated at 10% of the asset value or their actual AMC cost quoted after expiry of warranty period, whichever is higher, will be considered for the purpose of calculating LD.
- For repeat failure, same or higher LD will be charged depending upon the delay in rectification of the problem.
- LD will be calculated on Quarterly basis and deducted against the Quarterly payments.
- In case of CSOC operations failure, the LD will be charged for both CSOC Operations failure and individual security solution/device failure.

- For the L1, L2 and L3 resources for the leave of absence: - Each on-site resource shall be granted a maximum up to 01 (One) day leave per month. However, substitute should be provided. LD will be levied for any absence for which no substitute is arranged by the Service Provider as per defined in the below table. The LD charges will be in addition to the pro rata charges for the resources for their days of absence.

Resource Category	Liquidated Damages beyond leave of absence
Support Resources	<ul style="list-style-type: none"> L1 Resource - Rs.2000/- per day maximum Rs.10000/- per month L2 Resource - Rs.2500/- per day maximum Rs.15000/- per month L3 Resource - Rs 3000/- per day maximum Rs 20000/- per month

- VSCDL reserves right to recover / adjust the LD from any dues pending to the bidder.
- However, the maximum LD levied shall not be more than the 10% of total value of the order per quarter.
- If quarterly uptime of CSOC operations is less than 95%, VSCDL shall levy LD as above and shall have full right to issue notice & seek explanation under this RFP. The above LD shall be deducted from any payments due to the bidder.

8.1.3 SLA for Maintenance and Support Term

The SLAs for Maintenance and Support Term are modified as per the table given below:

S. No	Service Area	Service Level	Liquidated Damages
1	Monitoring, Analysis & Incident Reporting	<ul style="list-style-type: none"> 8x7x365 monitoring and reporting of all in-scope devices Categorization of events into Critical, High, Medium and Low priority shall be carried out in consultation with the selected bidder during the contracting period. All Critical, High and Medium priority events should be logged as incident tickets and responded as per SLA. Events along with action plan/mitigation steps should be 	<ul style="list-style-type: none"> Critical Events: - 3% of monthly CSOC Monitoring and Operations cost High Priority Events: - 2% of monthly CSOC Monitoring and Operations cost Medium/Low Priority Events: - 1% of the monthly CSOC Monitoring and Operations cost <p>Note: Operational Events need to be logged and maintained for reference.</p> <p>An incident ticket need not be raised for such incidents. However, these need to be included in the daily reports.</p>

		<p>alerted to designated VSCDL personnel as per the below SLA:</p> <ol style="list-style-type: none"> 1) Critical events within 15 minutes of the event identification. 2) High priority events within 30 minutes of the event identification. 3) Medium and Low priority events within 60 minutes of the event identification. 	
2	Incident Resolution	<p>For the devices/ solutions managed and administrated by the bidder</p> <ol style="list-style-type: none"> 1. Critical incidents within 60 minutes of the event Identification. 2. High priority incidents within 90 minutes of the event identification. 3. Medium priority incidents within 120 minutes of the event identification. 	<ul style="list-style-type: none"> • Critical Events: - 3% of monthly CSOC Monitoring and Operations cost • High Priority Events: - 2% of monthly CSOC Monitoring and Operations cost • Medium/Low Priority Events: - 1% of the monthly CSOC Monitoring and Operations cost <p>Note: operational incidents need to be logged and maintained for reference. These need to be included in the daily reports</p>
3	Security Breach	The system should be protected from all external security threats. The bidder shall ensure that there are no security breaches during the entire duration of the project	For every security breach the bidder shall incur a penalty of 10% of monthly CSOC Monitoring and Operations cost (OPEX)
4	Reports and Dashboard	<p>Daily Reports: Critical reports should be submitted on a daily basis by 11:00 AM</p> <p>Weekly Reports: By 11:00 AM, Monday</p> <p>Monthly Reports: 3rd working day of each month</p>	<ol style="list-style-type: none"> 1) Delay in reporting for daily report for more than 2 hours shall incur a liquidated damage of Rs. 100/- per hour, maximum of Rs. 1000/- per day 2) Delay in reporting by more than 2 days for both weekly and monthly reports shall incur a LD of Rs. 1500/- per day, maximum of Rs. 4500/- per month
4.	Vulnerability Assessment and Penetration Testing	The bidder shall carry out Vulnerability Assessment and Penetration Testing activity during implementation phase as well as	<ol style="list-style-type: none"> 1) For every week delay in submission of VAPT report, the bidder shall be liable to a penalty of 0.5% of VAPT cost 2) For every week delay in closure of vulnerabilities, the bidder shall be liable to a penalty of 0.5% of VAPT cost

		<p>yearly VAPT activity once every year during O&M period</p> <p>The bidder shall provide VAPT report within one month of the VAPT activity</p> <p>The bidder shall close all reported vulnerabilities in their proposed components in the same quarter as the VAPT activity</p>	
5	VAPT advisory & remediation services	<p>The bidder is expected to provide advisory-cum-remediation services for VAPT comments generated by internal and vulnerability assessment and penetration testing carried out by the Third-Party Cert-In empanelled agency</p> <p>Provide steps for fixing the vulnerabilities and/or suggest VSCDL's team of compensating controls that needs to be implemented in order to circumvent the vulnerability Implement the resolution in VSCDL's test setup. Upon getting VSCDL team's concurrence, proceed with production resolution. In the case of application dependencies, the details shall be provided, and compensating controls suggested, wherever possible</p>	<p>1. Delay in providing steps for fixing the critical vulnerabilities within 3 working days after reporting will incur Rs. 100 per vulnerability.</p> <p>2. Delay in providing steps for fixing the medium vulnerabilities within 7 working days after reporting will incur Rs. 300 per vulnerability</p> <p>3. Delay in providing steps for fixing the low vulnerabilities within 30 working days after reporting will incur Rs.500 per vulnerability</p>
6	Periodic Reviews	<p>The bidder is expected to improve the operations on an on-going basis.</p> <p>The bidder is expected to provide a quarterly report of the new improvements suggested, action plans, and the status of these improvements to VSCDL. The CSOC project sponsor or location delegate from the bidder is expected to conduct a quarterly review meeting with participating VSCDL officials resulting in a report covering details about current CSOC SLAs, status of operations, key threats and new threats identified, issues and challenges etc.</p>	<p>Quarterly meeting every quarter for the operations and maintenance phase. (If required, meeting will be done on monthly basis)</p> <p>A delay of more than two days will incur a LD of 1% of monthly CSOC Monitoring and Operations cost</p>

RFP for Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL
(Second Attempt)

7	Security (Threat) Intelligence Services	Advisories within 12 hours (considering 8x7x365 service window) of new global threats & vulnerabilities disclosures.	A delay of more than Two days will incur a LD of 1% of monthly CSOC Monitoring and Operations cost
8	New Patches	New patches for the items supplied by the bidder are applied within three days of them becoming generally available to all related technologies supplied by the bidder.	A delay of more than two days will incur a LD of 1% of monthly CSOC Monitoring and Operations cost
9.	Security Device Management and Administration	Bidder is expected to provide this service 8x7x365 basis. Management and administration of all security devices / solutions supplied under CSOC.	1. For more than 4 hours delay (after VSCDLs confirmation) for rule modification OR for wrong rule modification in any of the security devices / solutions will incur a LD of 1% of monthly CSOC Monitoring and Operations cost.

8.2 SLA Exclusions

- The time lost due to power or environmental failures not attributed to the bidder shall not be included in calculating “Resolution Time”
- In case of hardware damage by natural conditions and in case of theft of hardware vendor, shall not be responsible
- Maximum penalty, for not adhering to SLA requirement, that can be recovered as per rates mentioned above shall be 10% of the total contract price. Once the maximum is reached, client shall have the right to terminate the Contract without prejudice to its rights for claiming further general damages under the law.
- The downtime calculated shall not include the following:
 - Down time due to hardware/software and application which is owned by VSCDL at their premises
 - Negligence or other conduct of VSCDL, including a failure or malfunction resulting from applications or services provided by VSCDL or its other vendors
 - Failure or malfunction of any equipment or services not provided by the selected vendor
- However, it is the responsibility/onus of the selected bidder to prove that the outage is attributable to VSCDL. The selected vendor shall obtain the proof authenticated by the VSCDL’s official that the outage is attributable to the VSCDL.

Note:

- The selected vendor shall deploy sufficient manpower suitably qualified and experienced in shifts to meet the SLA. Selected vendor shall appoint as many team members as deemed fit by them, to meet the time schedule and SLA requirements.

8.3 Issue and Escalation Management Procedures

Issue Management process provides for an appropriate management structure towards orderly consideration and resolution of business and operational issues in the event of a quick consensus not reached between the VSCDL and the selected vendor. Implementing such a process at the commencement of services shall significantly improve the probability of successful issue resolution. It is expected that this pre-defined process will only be used on an exception basis if issues are not resolved at operational levels.

8.4 Issue Management Procedures

Either the VSCDL or the selected vendor may raise an issue by documenting the business or technical problem, which presents a reasonably objective summary of both points of view and identifies specific points of disagreement with possible solutions.

- The VSCDL and the selected vendor will determine which committee or executive level should logically be involved in resolution. A chain of management escalation is defined for the same.
- A meeting or conference call will be conducted to resolve the issue in a timely manner. The documented issues will be distributed to the participants at least 24 hours prior to the discussion if the issue is not an emergency requiring immediate attention.
- The VSCDL and the selected vendor shall develop an interim solution, if required, and subsequently the permanent solution for the problem at hand. The selected vendor will then communicate the resolution to all interested parties.
- In case the issue is still unresolved, the arbitration procedures described in the Contract will be applicable.

8.5 SLA Change Control

It is acknowledged that this SLA may change as VSCDL's business needs evolve over the course of the Contract period. This document also defines the following management procedures:

1. A process for negotiating changes to the SLA
2. An issue management process for documenting and resolving difficult issues
3. VSCDL and selected vendor management escalation process to be used in the event that an issue is not being resolved in a timely manner by the lowest possible level of management

Any changes to the levels of service provided during the term of this Agreement will be requested, documented and negotiated in good faith by both parties. Either party can request a change. Changes will be documented as an addendum to this SLA and, subsequently, the Contract.

If there is any confusion or conflict between this document and the Contract, the Tender and its addenda, the Contract will supersede.

8.6 SLA Change Process

The parties may amend this SLA by mutual agreement in accordance with terms of this contract. Changes can be proposed by either party. The selected vendor can initiate an SLA review with the VSCDL. Unresolved issues will be addressed using the issue management process described in this document. The selected vendor shall maintain and distribute current copies of the SLA document as directed by VSCDL. Additional copies of the current SLA will be made available at all times to authorized parties.

8.7 Version Control

All negotiated SLA changes will require changing the version control number. As appropriate, minor changes may be accumulated for periodic release (e.g. every month) or for release when a critical threshold of change has occurred.

8.8 Responsibilities of the Parties

8.8.1 Responsibilities of the Selected Vendor

Selected vendor is responsible for executing this Contract and delivering the services, while maintaining the specified performance targets.

Additionally the selected vendor is responsible for:

- Reporting problems to VSCDL as soon as possible
- Assisting VSCDL in management of the SLA
- Providing early warning of any organizational, functional or technical changes that might affect selected vendor's ability to deliver the services
- Assisting VSCDL to address and resolve issues from time to time

Selected vendor shall take immediate action to identify problems and follow up with appropriate action to fix them as quickly as possible.

8.8.2 Responsibilities of the VSCDL

VSCDL is responsible for:

- Reporting defects and problems to the selected vendor as soon as possible
- Assisting selected vendor in management of the SLA
- Providing early warning of any organizational, functional or technical changes that might affect selected vendor's ability to deliver the services
- Assisting selected vendor to address and resolve issues from time to time

Selected vendor shall take immediate action to identify problems and follow up with appropriate action to fix them as quickly as possible.

8.9 Management Escalation Procedures and Contact Map

The purpose of this escalation process is to provide a quick and orderly method of notifying both parties that an issue is not being successfully resolved at the lowest possible management level. Implementing this procedure would mean that VSCDL and selected vendor management are communicating at the appropriate levels.

Escalation Procedure

Escalation should take place on an exception basis and only if successful issue resolution cannot be achieved in a reasonable time frame.

- Either the VSCDL or the selected vendor can initiate the procedure
- The "moving party" should promptly notify the other party that management escalation will be initiated
- Management escalation will be defined as shown in the contact map below
- Escalation will be one level at a time and concurrently

Contact Map

Escalation Level	Department Representative with Contact Details	Selected Vendor* Representative with Contact Details
Level 1: Project Manager		
Level 2: Steering Committee		

***Selected vendor shall provide Detailed CVs for the following:**

- a) Project Manager/CSOC Lead
- b) Team Members

9 Annexure I: Instructions for Pre-Qualification Bid

9.1 Pre-Qualification Cover Letter

Date: <DD/MM/YYYY>

To,

CEO, Vadodara Smart City Development Limited (VSCDL)

Sub : Selection of SI for the Project " Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)"

Ref : Tender No: <No> dated <DD/MM/YYYY>

Dear Sir,

Having examined the Bid document (and the clarification / corrigendum issued thereafter, if any), the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide the professional services as required and outlined in the Bid document for the " **Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)**".

We attach hereto our responses to pre-qualification requirements and technical & commercial proposals as required by the RFP. We confirm that the information contained in these responses or any part thereof, including the exhibits, and other documents and instruments delivered or to be delivered to VSCDL, is true, accurate, verifiable and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part mislead the department in its shortlisting process.

We fully understand and agree to comply that on verification, if any of the information provided here is found to be misleading the selection process, we are liable to be dismissed from the selection process or termination of the contract during the project, if selected to do so.

We agree for unconditional acceptance of all the terms and conditions set out in the RFP (and subsequent clarification/corrigendum, if any) document and also agree to abide by this tender response for a period of 180 days from the date fixed for bid opening. We hereby declare that in case the contract is awarded to us, we shall submit the contract performance guarantee bond in the form prescribed the RFP.

We agree that you are not bound to accept any tender response you may receive. We also agree that you reserve the right in absolute sense to reject all or any of the products/ services specified in the tender response.

It is hereby confirmed that I/We are entitled to act on behalf of our company/ corporation/ firm/ organization and empowered to sign this document as well as such other documents, which may be required in this connection.

Signature of Authorized Signatory (with official seal)

Name :
Designation :
Company :
Address :
Telephone & Fax :
E-mail Address :

9.2 Check-list for the documents to be included in the Pre-Qualification Folder

#	Documents to be submitted	Submitted (Y / N)	Documentary Proof (Page No.)
1.	DD of required amount as Tender fee (in separate envelop)		
2.	EMD of INR 20,00,000/- (Rupees Twenty Lakhs only) (Form PQ_1)		
3.	Bid Cover Letter		
4.	Power of Attorney/board resolution to the authorized signatory of the bid		
5.	Copy of certificate of incorporation		
6.	Certificate from the statutory auditor/CA specifying the (a) Annual turnover for last 3 audited financial years (FY 2016-17, 2017-18 and 2018-19), (b) Annual turnover from Information Technology business in India for last 3 audited financial years (FY 2016-17, 2017-18 and 2018-19), (c) Annual turnover from Information Security/Cyber Security Business for last 3 audited financial years (FY 2016-17, 2017-18 and 2018-19), (d) Net worth as on 31 st march 2019		
7.	Details of the projects executed (Form PQ_5 and PQ_6) along with <ul style="list-style-type: none"> Copy of Work Order of the project from the client clearly depicting the scope of work, contract period, BOQ and project value. Copy of Contract Copy of Work Completion Certificate from the client Client contact details with Mobile number, Landline number and Email ID <p>Note: Form PQ_5 needs to be used to cite the project details for PQ clause 5 & 6 of the RFP</p>		
8.	Declaration that the firm is not blacklisted by Central Government or any State Government organization/ department in India at the time of submission of the bid (Form PQ_7)		
9.	Declaration on stamp paper, for bidder not terminated, not being insolvent or in receivership or bankrupt (Form PQ_8)		

RFP for Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL
(Second Attempt)

#	Documents to be submitted	Submitted (Y / N)	Documentary Proof (Page No.)
10.	Copy of audited balance sheet for last three financial years 2016-17, 2017-18 and 2018-19		
11.	Copy of the audited profit & loss statements for last three financial years 2016-17, 2017-18 and 2018-19		
12.	Copy of valid GST registration certificate		
13.	Copy of PAN card along with documentary proof of Income Tax returns for the last three financial years i.e. 2016-17, 2017-18, 2018-19.		
14.	Valid copy of certifications as asked PQ Clause		
15.	Certificate from HR head confirming compliance as per PQ clause		

9.3 PQ_1: Bank Guarantee for Earnest Money Deposit (EMD)

To,

<Name>
<Designation>
<Address>
<Phone No.>
<Fax No.>
<Email ID>

Whereas <<name of the bidder>> (hereinafter called 'the Service Provider') has submitted the bid for submission of Tender <<tender number>> dated <<date>> for <<name of the assignment>> (hereinafter called "the Bid") to <<name of purchaser>>.

Know all Men by these presents that we <<name of company>> having our office at <<address>> (hereinafter called "SI") are bound unto the << purchaser >> (hereinafter called "the Purchaser") in the sum of INR <<amount in figures>> (Rupees <<amount in words>> only) for which payment well and truly to be made to the said Purchaser, the SI binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this <<date>>.

The conditions of this obligation are:

1. If the bidder having its bid withdrawn during the period of bid validity specified by the Bidder on the Bid Form; or
2. If the bidder, having been notified of the acceptance of its bid by the Purchaser during the period of validity of bid
 - a. Withdraws his participation from the bid during the period of validity of bid document; or
 - b. Fails or refuses to participate in the subsequent Tender process after having been short listed;

We undertake to pay to the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to <<date>> and including <<extra time over and above mandated in the RFP>> from the last date of submission and any demand in respect thereof should reach VSCDL not later than the above date.

NOTWITHSTANDING ANYTHING CONTAINED HEREIN:

- I. Our liability under this Bank Guarantee shall not exceed INR <<amount in figures>> (Rupees <<amount in words>> only)
- II. This Bank Guarantee shall be valid up to <<date>>
- III. It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this Bank Guarantee that we receive a valid written claim or demand for payment under this Bank Guarantee on or before <<date>> failing which our liability under the guarantee will automatically cease.

(Authorized Signatory of the Bank)

Seal:

Date:

9.4 PQ_2: Bidder Information Format

<<To be printed on Bidder Company's Letterhead and signed by Authorized Signatory>>

To,

CEO, Vadodara Smart City Development Limited (VSCDL)

Subject: "Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)".

Dear Sir,

Please find below details for participation in "Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)" tender.

Bidder Information Sheet		
#	Particulars	Bidder
1.	Name of the Organization	
2.	Website	
3.	Type of Organization (Pvt. Ltd./Public Limited/LLP)	
4.	Address of Registered Office	
5.	Company Registration Details	
6.	Date of Registration	
7.	Details of any Global Certifications (ISO/CMMi etc.)	
8.	Details of Company PAN Card t	
9.	GST Registration Number and Certificate	
10.	Address of Registered Office in India	
11.	No. of Years of Operation in India	
12.	Authorized Signatory Name	
13.	Authorized Signatory Designation	
14.	Authorized Signatory Contact Mobile Number and Email	

Yours sincerely,

Signature of Authorized Signatory (with official seal)

Name :

Designation :

Address :

Telephone & Fax :

E-mail Address :

Note: To be submitted with any other supporting details specified as document proof in Section 3.4

9.5 PQ_3: Power of Attorney

Whereas the VSCDL has invited applications from interested parties for the **“Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)”**.

Whereas _____ interested in bidding for the project in accordance with the terms and conditions of the Request for Proposal (RFP document) and other connected documents in respect of the Project, and

NOW, THEREFORE, KNOW ALL MEN BY THESE PRESENTS

M/s _____ having our registered office at _____,

AND hereby agree to ratify and confirm and do hereby ratify and confirm all acts, deeds and things done or caused to be done by our said Attorney pursuant to and in exercise of the powers conferred by this Power of Attorney and that all acts, deeds and things done by our said Attorney in exercise of the powers hereby conferred shall and shall always be deemed to have been done by us.

IN WITNESS WHEREOF WE THE PRINCIPALS ABOVE NAMED HAVE EXECUTED THIS POWER OF ATTORNEY ON THIS _____ DAY OF _____, 20____

For _____
(Signature)

(Name & Title)

For _____
(Signature)

(Name & Title)

For _____
(Signature)

(Name & Title)

Witnesses:

- 1.
- 2.

(Executants)

Notes:

- *The mode of execution of the Power of Attorney should be in accordance with the procedure, if any, laid down by the applicable law and the charter documents of the executant(s) and when it is so required, the same should be under common seal affixed in accordance with the required procedure.*
- *Also, wherever required, the Bidder should submit for verification the extract of the charter documents and documents such as a board or shareholders' resolution/power of attorney in favour of the person executing this Power of Attorney for the delegation of power hereunder on behalf of the Bidder.*
- *For a Power of Attorney executed and issued overseas, the document will also have to be legalized by the Indian Embassy and notarized in the jurisdiction where the Power of Attorney is being issued. However, the Power of Attorney provided by Bidders from countries that have signed The Hague Legislation Convention, 1961 are not required to be legalized by the Indian Embassy if it carries a conforming Apostille certificate.*

9.6 PQ_4: Bidder's Turnover Details and Net Worth

<<To be printed on Bidder Company's Letterhead and signed by Authorized Signatory>>

<<The same format to be used for CA Certificate >>

Date: DD/MM/YYYY

To,

CEO, Vadodara Smart City Development Limited (VSCDL)

Subject: "Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)".

Dear Sir,

I have carefully gone through the Terms & Conditions contained in the RFP document for **"Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)"**. I hereby declare that below are the financial details of our organization for last 3 financial years (FY 2016-17, 2017-18 and 2018-19).

SI No.	Details	FY 2016-17 (i)	FY 2017-18 (ii)	FY 2018-19 (iii)	Average [(i)+(ii)+(iii))/+3]
1	Annual turnover for last 3 audited financial years				
2	Annual turnover from Information Technology business in India for last 3 audited financial years				
3	Annual turnover from Information Security/Cyber Security Business				
4	Net worth (As on 31-03-2019)	NA	NA	NA	

Contact details of officials for future correspondence regarding the bid process:

Details	Authorized Signatory	Secondary Contact
Name		
Title		
Company Address		

RFP for Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)

Mobile		
Fax		

I further certify that I am competent officer in my company to make this declaration.

Yours sincerely,

Signature of Authorized Signatory (with official seal)

Name :
Designation :
Address :
Telephone & Fax :
E-mail Address :

Note: To be submitted with any other supporting details specified as document proof in Section 3.4

9.7 PQ_5: Experience of Implementing Cyber security /CSOC related projects

<<To be printed on Company's Letterhead and signed by Authorized Signatory>>

Date: DD/MM/YYYY

To,

CEO, Vadodara Smart City Development Limited (VSCDL)

Dear Sir,

I have carefully gone through the Terms & Conditions contained in the RFP document for “**Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)**”. I hereby declare that below are the details regarding relevant work that has been taken up by our company and matching with the pre-qualification criteria asked in section 3.4

Name of the Project	Project 1	Project 2	Project 3	-	Project n
General Information					
Client for which the project was executed					
Name of the client contact person(s)					
Designation of client contact person(s)					
Contact details of the client contact person(s) (Email, Landline and Mobile numbers)					
Project Details					
Description of the project					
Scope of work of the bidder					
Deliverables of the bidder					
List and Summary of Cyber Security Equipment/ Solutions used					
Other Details					
Total cost of the project					

RFP for Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL
(Second Attempt)

Name of the Project	Project 1	Project 2	Project 3	-	Project n
(If project is executed as a consortium member, then provide cost of work done as per scope of work allocation only)					
Duration of the project (number of months, start date, completion date, current status)					
Other relevant information <for each type of the project type>					
Mandatory Supporting Documents					
LoI/work order with full BoQ					
Contract agreement					
Copy of invoice submitted to the client					
Client certificate giving present status of the project and view of the quality of services by the bidder					

I further certify that I am competent officer in my company to make this declaration.

Yours sincerely,

Signature of Authorized Signatory (with official seal)

Name :
Designation :
Address :
Telephone & Fax :
E-mail Address :

Note: To be submitted with any other supporting details specified as document proof in Section 6.

9.8 PQ_6: Undertaking for Technically Qualified Full-time Professionals on Company's Payroll

<<To be printed on Company's Letterhead and signed by Authorized Signatory>>

Date: DD/MM/YYYY

To,

CEO, Vadodara Smart City Development Limited (VSCDL)

Dear Sir,

I have carefully gone through the Terms & Conditions contained in the RFP document for “**Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)**”. I hereby declare that my company <company's name> has <number > technically qualified professionals as on 31 March 2018.

NOTE: To be filled for the bidder

#	Name of the Resource	Proposed Role	Highest Qualification	Total Experience (in years)	Total Relevant Experience for the Proposed Position (in Years)	Certifications
1.						
2.						
3.						
4.	...					

I further certify that I am competent officer in my company to make this declaration.

Yours sincerely,

Signature of Authorized Signatory (with official seal)

Name :

Designation :

Address :

Telephone & Fax :

E-mail Address :

Note: To be submitted with any other supporting details specified as document proof in Section 7.22.

9.9 PQ_7: Self Declaration – No Blacklisting

<<To be printed on INR 300/- Stamp Paper>>

Date: DD/MM/YYYY

To,

CEO, Vadodara Smart City Development Limited (VSCDL)

Dear Sir,

In response to the Tender Ref. No. _____ dated _____ for
“Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)”, as an Owner/Partner/Director of _____, I/We hereby declare that presently our Company/Firm _____ is having unblemished record and is not declared ineligible for corrupt and fraudulent practices either indefinitely or for a particular period of time by any State/Central Government/PSU.

We further declare that presently our Company/Firm _____ is not blacklisted and not declared ineligible for reasons other than corrupt and fraudulent practices by any State/Central Government/PSU on the date of bid submission.

If this declaration is found to be incorrect then without prejudice to any other action that may be taken, my/ our security may be forfeited in full and the tender if any to the extent accepted may be cancelled.

Yours sincerely,

Signature of Authorized Signatory (with official seal)

Name :

Designation :

Address :

Date :

Place :

Seal of the Organization :

9.10 PQ_8: Self Declaration – Bidder Not Terminated, Not Being Insolvent or In Receivership or Bankrupt

<<To be printed on INR 300/- Stamp Paper>>

Date: DD/MM/YYYY

To,

CEO, Vadodara Smart City Development Limited (VSCDL)

Dear Sir,

In response to the Tender Ref. No. _____ dated _____ for **“Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)”**, as an Owner/Partner/Director of _____, I/We hereby declare that presently our Company/Firm _____:

- a) has not been terminated by any Government/Semi-Government or Public Authority or Public Institution in India or abroad, before the completion of respective Contract period for which it has executed the project or in process of execution of such project, on account of its poor performance, delay or abandonment of work by it
- b) is not insolvent, in receivership, bankrupt or being wound up, not have its affairs administered by a court or a judicial officer, not be declared defaulter by any financial institution, not have its business activities suspended and must not be the subject of legal proceedings for any of the foregoing reasons
- c) not has, and their directors and officers not have, been convicted of any criminal offence related to their professional conduct or the making of false statements or misrepresentations as to their qualifications to enter into a procurement contract within a period of three years preceding the commencement of the procurement process, or not have been otherwise disqualified pursuant to debarment proceedings
- d) does not have a conflict of interest in the procurement in question as specified in the RFP

If this declaration is found to be incorrect then without prejudice to any other action that may be taken, my/ our security may be forfeited in full and the tender if any to the extent accepted may be cancelled.

Yours sincerely,

Signature of Authorized Signatory (with official seal)

Name :

Designation :

Address :

Date :

Place :

Seal of the Organization :

10 Annexure II: Instructions for Technical Bid

10.1 General Instructions for Preparation of the Technical Proposal

- i. Bidders have to submit a very structured and organized technical bid, which will be analysed by the Technical Evaluation Committee for different compliances with regards to the requirements of the project. The document submitted must be searchable and well indexed without any handwritten material. Since the cut-off marks for Technical bid Score is 70, the quality and completeness of the information submitted by the bidder will matter a lot. All the documents must be submitted in one file only.
- ii. Bidder is expected to divide its bid in following sections/documents:

a. Bidder's Competence to Execute the Project

This document should bring about the capability of the firm to execute this project. Some of the required documents are as follows:

- Financial capability of the bidder in required formats and supporting documents
- Experience of executing similar projects

b. Technical Proposal

The technical proposal should specify the following:

- Understanding of the project
- Clear articulation and description of the design and technical solution and various components including (infrastructure architecture, application architecture, data architecture and physical street layer architecture)
- Details of the all Cyber Security Solutions proposed
- Integration approach with existing infrastructure
- Reasoning for selection of the proposed technology over other options
- Strength of the bidder to provide services including examples or case-studies of similar solutions deployed for other clients
- Clearly articulate the strategy and approach & methodology for design, installation, configuration and maintenance of project components, data recovery and hosting infrastructure of the project.
- Approach and Methodology for management of SLA requirements specified in the bid. Bidder is required to clearly articulate how the SLA requirements would be adhered.
- Detailed Project Plan with timelines, resource allocation, milestones etc. for supply, installation and commissioning of the various project components.
- The Operations and Risk Mitigation plan.

c. Other Details

- **Bill of Material & BoQ:** The bidder should give details of all the proposed IT and Non-IT components, without specifying the costs in the format given below. Please note that the bid shall get disqualified if Bidder gives price details in the technical document.

#	Name of Item	OEM/ Make	Exact Model	Part No.	Quantity/ License Count Offered
1.	<Item 1>				
2.	<Item 2>				
3.	<Item 3>				

4.	<Item 4>				
----	----------	--	--	--	--

- Make and Model (one & only one unique Make and Model per BOQ item is required) of all IT as well as Non-IT components along with datasheets highlighting Technical Specification parameters in each datasheet for compliances.
- Compliance to Technical and Functional specifications as mentioned against each specification feature.
- CVs of the Key Manpower proposed (Qualification of each resource is provided)

d. OEM Details

- For OEM selection criteria, please refer Annexure XX.
- During the Presentation/Demonstration at technical evaluation stage, the Technical Committee will give special attention to verify the quality, robustness and appropriateness of the proposed equipment/components. If any brand/product is found unsuitable, bidder may get disqualified or may be asked to replace the product with better brands meeting the tender requirements. Without any cost implication or change s in commercial bid.

e. Proposed Team for the Project

- As specified in Technical Bid Evaluation Framework, VSCDL would give importance to the right people proposed for the project. Bidder may propose different people for different skill-sets required and different responsibilities (during project implementation and post-implementation). Following documentation is expected in this section:
 - (a) Overall project team (for both Implementation and Post Implementation support phases)
 - (b) Escalation chart for the entire project duration
 - (c) Summary table providing qualification, experiences, certifications and other relevant details
 - (d) Detail CVs in the format attached
- All above mentioned documents shall have an index page with page numbers specified for all the key information/headers on company's cover letter.
- During the demo at technical evaluation stage, the Technical Committee will give special attention to verify the quality, robustness and appropriateness of the proposed equipment/components for city

10.2 Documents Checklist for Technical Bid

#	Documents to be submitted	Submitted (Y / N)	(Page No.)
1.	Bidder competence related docs (Form TQ_1)		
2.	Details of projects executed (Form TQ_2 and TQ_3)		
3.	Understanding of the project		
4.	Description of the design and technical solution and various components including (Cyber security solution/ infrastructure architecture, application architecture, Information security architecture, etc)		
5.	Details of the cyber security solutions offered <ul style="list-style-type: none"> • NG Firewall (External) (1+1 in HA mode) • Web Application Firewall solution • Additional AV Licenses for Servers • Additional AV Licenses for Desktops • SIEM solution • PIM Solution • Server Security (HIPS) (For servers) • DLP Solution (End point, Web, Network, File Share) • Anti APT Solution • NAC (Network Access Control) Solution • 2 Factor Authentication 		
6.	Integration approach with existing infrastructure including existing IT security solution/devices		
7.	Reasoning for selection of the proposed technology over other options		
8.	Strength of the bidder to provide services including examples or case-studies of similar solutions deployed for other clients		
9.	Approach and methodology for design, installation, configuration and maintenance of cyber security components		
10.	Approach and methodology for Design, implementation and operations of Centralized Security Operations Centre		
11.	Approach and methodology for Preparation and Implementation of Cyber Security Framework and Policy		
12.	Approach and methodology for management of SLA requirements specified in the bid. Bidder is required to clearly articulate how the SLA requirements would be adhered.		
13.	Detailed project plan with timelines, resource allocation, milestones etc. for supply, installation and commissioning of the various project components		
14.	Network bandwidth requirement for the operations		
15.	Risk mitigation plan		
16.	Technically qualified full-time professionals (Form TQ_3)		
17.	Manpower deployed on the project (Form TQ_4) for implementation and O&M phase		

RFP for Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL
(Second Attempt)

#	Documents to be submitted	Submitted (Y / N)	(Page No.)
18.	CVs of the manpower proposed (Form TQ_5)		
19.	Make, model, quantities and licence count (complete bill of material, without price) for all cyber security components		
20.	Compliance to Technical & Functional specifications asked in RFP/Corrigendum		
21.	Datasheets highlighting the Technical specification parameters in each datasheet for compliances		
22.	Authorization letters from all OEMs (Form TQ_6)		

10.3 TQ_1: Bidder's Turnover Details and Net Worth

<<To be printed on Bidder Company's Letterhead and signed by Authorized Signatory>>

<<The same format to be used for CA Certificate >>

Date: DD/MM/YYYY

To,

CEO, Vadodara Smart City Development Limited (VSCDL)

Subject: "Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)".

Dear Sir,

I have carefully gone through the Terms & Conditions contained in the RFP document for **"Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)"**. I hereby declare that below are the financial details of our organization for last 3 financial years (FY 2016-17, 2017-18 and 2018-19).

SI No.	Details	FY 2016-17 (i)	FY 2017-18 (ii)	FY 2018-19 (iii)	Average [(i)+(ii)+(iii))/+3]
1	Annual turnover for last 3 audited financial years				
2	Annual turnover from Information Technology business in India for last 3 audited financial years				
3	Annual turnover from Information Security/Cyber Security Business				
4	Net worth (As on 31-03-2019)	NA	NA	NA	

Contact details of officials for future correspondence regarding the bid process:

Details	Authorized Signatory	Secondary Contact
Name		
Title		
Company Address		

RFP for Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL
(Second Attempt)

Mobile		
Fax		

I further certify that I am competent officer in my company to make this declaration.

Yours sincerely,

Signature of Authorized Signatory (with official seal)

Name :
Designation :
Address :
Telephone & Fax :
E-mail Address :

Note: To be submitted with any other supporting details specified as document proof in Section 3.4

10.4 TQ_2: Experience of Implementing IT/ICT Projects

<<To be printed on Company's Letterhead and signed by Authorized Signatory>>

Date: DD/MM/YYYY

To,

CEO, Vadodara Smart City Development Limited (VSCDL)

Dear Sir,

I have carefully gone through the Terms & Conditions contained in the RFP document for “**Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)**”. I hereby declare that below are the details regarding relevant work that has been taken up by our company

NOTE: To be filled separately for each project undertaken by the bidder

Name of the Project	Bidder				
	Project 1	Project 2	Project 3	-	Project n
General Information					
Client for which the project was executed					
Name of the client contact person(s)					
Designation of client contact person(s)					
Contact details of the client contact person(s)					
Project Details					
Description of the project					
Scope of work of the bidder					
Deliverables of the bidder					
Technologies used					
Other Details					
Total cost of the project					
(If project is executed as a consortium member, then provide cost of work done as per scope of work allocation only)					
Duration of the project (number of months, start date, completion date, current status)					
Other relevant information <for each type of the project type>					
Mandatory Supporting Documents					
LoI/work order with full BoQ					
Contract agreement					
Copy of invoice submitted to the client					
Client certificate giving present status of the project and view of the quality of services by the bidder					

I further certify that I am competent officer in my company to make this declaration.

Yours sincerely,

Signature of Authorized Signatory (with official seal)

Name :
Designation :
Address :
Telephone & Fax :
E-mail Address :

Note: To be submitted with any other supporting details specified as document proof in Section 7.22
.

10.5 TQ_3: Undertaking for Technically Qualified Full-time Professionals on Company's Payroll

<<To be printed on Company's Letterhead and signed by Authorized Signatory>>

Date: DD/MM/YYYY

To,

CEO, Vadodara Smart City Development Limited (VSCDL)

Dear Sir,

I have carefully gone through the Terms & Conditions contained in the RFP document for “**Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)**”. I hereby declare that my company <company's name> has <number > technically qualified professionals as on 31 March 2017.

#	Name of the Resource	Proposed Role	Highest Qualification	Total Experience (in years)	Total Relevant Experience for the Proposed Position (in Years)	Certifications
1.						
2.						
3.						

I further certify that I am competent officer in my company to make this declaration.

Yours sincerely,

Signature of Authorized Signatory (with official seal)

Name :

Designation :

Address :

Telephone & Fax :

E-mail Address :

Note: To be submitted with any other supporting details specified as document proof in Section 7.22.

10.6TQ_4: Undertaking for Manpower Deployed on Project

<<To be printed on Company's Letterhead and signed by Authorized Signatory>>

Date: DD/MM/YYYY

To,

CEO, Vadodara Smart City Development Limited (VSCDL)

Dear Sir,

I have carefully gone through the Terms & Conditions contained in the RFP document for “**Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)**”. I hereby declare that following resources are being proposed for the project.

Implementation Period

#	Proposed Position	Resource Name (s)	Proposed CV Compliance
1.	Project Manager		
2.	<< Position 1>>		
3.	<< Position 2>>		
4.	<< Position N>>.....		

O&M Period

#	Proposed Position	Resource Name(s)	Proposed CV Compliance
1.	SOC Lead -cum - CISO		
2.	L3 - Enterprise Application Security Professional		
3.	L2 - Data Protection Analysts IoT / Endpoint Security		
4.	L1 - IT Analysts / Auditor		

I further certify that I am competent officer in my company to make this declaration.

Yours sincerely,

Signature of Authorized Signatory (with official seal)

Name :
Designation :
Address :
Telephone & Fax :
E-mail Address :

Note: To be submitted with any other supporting details specified as document proof in Section 7.22.

10.7 TQ_5: CVs of the Manpower Proposed

<<CV of the proposed Manpower to be submitted in the following format>>

1.	Name of the Staff				
2.	Current Designation in the Organization				
3.	Proposed Role in the Project				
4.	Proposed Responsibilities in the Project				
5.	Date of Birth				
6.	Education	Degree/Diploma	College/University	Year of Passing	
7.	Key Training and Certifications				
8.	Language Proficiency	Language	Reading	Writing	Speaking
9.	Employment Record (For the Total Relevant Experience)	From /To	Employer	Position Held	
10.	Total No. of Years of Work Experience				
11.	Total No. of Years of Experience for the Role Proposed				

12.	Highlights of Relevant Assignments Handled and Significant Accomplishments	Use following format for each project														
		<table><tr><td>Name of Assignment/Project:</td><td></td></tr><tr><td>Year:</td><td></td></tr><tr><td>Location:</td><td></td></tr><tr><td>Client:</td><td></td></tr><tr><td>Main Project Features:</td><td></td></tr><tr><td>Positions Held:</td><td></td></tr><tr><td>Activities Performed:</td><td></td></tr></table>	Name of Assignment/Project:		Year:		Location:		Client:		Main Project Features:		Positions Held:		Activities Performed:	
Name of Assignment/Project:																
Year:																
Location:																
Client:																
Main Project Features:																
Positions Held:																
Activities Performed:																

10.8TQ_6: Format for Authorization Form (MAF) from OEMs

<<To be printed on OEM's Letterhead and signed by Authorized Signatory of OEM>>

Date: DD/MM/YYYY

To,

CEO, Vadodara Smart City Development Limited (VSCDL)

Subject: "Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)" – Authorization Letter from OEMs.

Reference: Tender No: <No> dated <DD/MM/YYYY>

Dear Sir,

We _____, (name and address of the manufacturer) who are established and reputed manufacturers of _____ having factories at _____ (addresses of manufacturing/development locations) do hereby authorize M/s _____ (name and address of the bidder) to bid, negotiate and conclude the contract with you against the above mentioned tender for the above equipment/software manufactured/developed by us.

We herewith certify that the above mentioned equipment/software products are not end of the life and we hereby undertake to support them for the duration of minimum 5 years from the date of this letter. We duly authorize the said firm to act on our behalf in fulfilling all installations, Technical support and maintenance obligations required by the contract.

We also confirm that we will ensure all product upgrades (including management software upgrades and new product feature releases) are provided by M/sfor all the products quoted for and supplied to VSCDL during the product warranty and AMC period.

We hereby declare that we are not insolvent, in receivership, bankrupt or being wound up, our affairs are not being administered by a court or a judicial officer, our business activities have not been suspended and we are not the subject of legal proceedings for any of the foregoing.

This authorisation letter shall be valid till the bid validity period defined in the RFP.

Yours faithfully,

(Signature of the Authorized Signatory of OEM)

Name:

Designation:

Seal:

Date:

Place:

Business Address:

(Signature of the Authorized Signatory of the Bidder)

Name:

Designation:

Seal:

Date:

Place:

Business Address:

11 Annexure III: List of Products/Solutions which require MAF from OEMs

The bidder shall submit Manufacturers Authorization Certificate (MAF) from Original Equipment Manufacturers (OEMs) of the following products/solutions:

Sr.	Equipment	MAF	Proof of OEM's existence in India
1	NG Firewall (External) (1+1 in HA mode)		
2	Web Application Firewall solution		
3	Additional Licenses for Servers		
4	Additional Licenses for Desktops		
5	SIEM solution		
6	IDAM Solution		
7	PIM Solution		
8	Server Security (HIPS) (For servers)		
10	DLP Solution (End point, Web, Network, File Share)		
11	Anti APT Solution		
12	NAC (Network Access Control) Solution		
13	2 Factor Authentication		
14	Cybersecurity Solutions for DR Site		

12 Annexure IV: Commercial Proposal Formats

12.1 Commercial Proposal Cover Letter

Date: <DD/MM/YYYY>

To

CEO, Vadodara Smart City Development Limited (VSCDL)

Vadodara Municipal Corporation

Khanderao Market, Vadodara – 390001, Gujarat

Sub : RFP for the Project " Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)"

Ref : Tender No: <No> dated <DD/MM/YYYY>

Dear Sir,

We, the undersigned Bidders, having read and examined in detail all the bidding documents in respect of **“Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)”** do hereby propose to provide services as specified in the RFP referred above.

1. PRICE AND VALIDITY

- All the prices mentioned in our Tender are in accordance with the terms as specified in the Tender documents. All the prices and other terms and conditions of this Tender are valid for a period of 2 years from the date of opening of the Tenders.
- We hereby confirm that our Tender prices include all taxes. Taxes are quoted separately under relevant sections, as specified in the RFP formats.
- We have studied the clause relating to Indian Income Tax and hereby declare that if any income tax, surcharge on Income Tax, Professional and any other corporate Tax is altered under the law, we shall pay the same.

2. UNIT RATES

We have indicated in the relevant schedules enclosed, the unit rates for the purpose of on account of payment as well as for price adjustment in case of any increase to / decrease from the scope of work under the contract.

3. DEVIATIONS

We declare that all the services shall be performed strictly in accordance with the RFP documents and there are no deviations except for those mentioned in Pre-Qualification Envelope, irrespective of whatever has been stated to the contrary anywhere else in our bid.

Further, we agree that additional conditions, if any, found in our bid documents, other than those stated in the deviation schedule in Pre-Qualification Envelope, shall not be given effect to.

4. QUALIFYING DATA

We confirm having submitted the information as required by you in your Instruction to Bidders. In case you require any other further information/documentary proof in this regard before evaluation of our Tender, we agree to furnish the same in time to your satisfaction.

5. BID PRICE

We declare that our Bid Price is for the entire scope of the work as specified in the RFP document. These prices are indicated in the subsequent sub-sections of this Section.

6. CONTRACT PERFORMANCE GUARANTEE BOND

We hereby declare that in case the contract is awarded to us, we shall submit the contract Performance Bank Guarantee in the form prescribed in the RFP.

We hereby declare that our Tender is made in good faith, without collusion or fraud and the information contained in the Tender is true and correct to the best of our knowledge and belief.

We understand that our Tender is binding on us and that you are not bound to accept a Tender you receive. We confirm that no Technical deviations are attached here with this commercial offer.

Yours Sincerely,

(Signature of the Authorised Signatory)

Name :

Designation :

Company :

Seal :

Date :

Place :

Address :

12.2 Commercial Bid Formats

General Instructions:

1. The bidder should provide all prices as per the prescribed format under this Annexure. Bidder should not leave any field blank. In case the field is not applicable, bidder must indicate “o” (Zero) in all such fields.
2. All types of taxes and duties must be added in tax columns to depict the different taxes involved for the various price schedule. VSCDL shall take into account all Taxes, Duties and Levies for the purpose of Evaluation.
3. Any changes in Govt. Taxes/Duties would be applicable as on actual at the time of invoice processing.
4. All the prices (even for taxes) are to be entered in Indian Rupees ONLY (%age values are not allowed)
5. VSCDL at its discretion may add/reduce the quantity of any item at the time of placing work order/ agreement and payment will be released on actual basis.
6. IT Infrastructure (Hardware) and other line items mentioned in these Schedule are indicative. Bidders to specify the actual ones. If any of the items are not required/not offered in solution, proper justification should be given in un-priced Bill of Material in the Technical Proposal.
7. The bidders are required to carry out due diligence in proposing various systems and keep in mind the overall system requirements and provide justification for the quantities in the Technical Proposal.
8. VSCDL reserves the right to question the logic of pricing for all the three years Cyber Security and other software as well as CAMC of specified years for Hardware, and thus bidders are required to ensure that no unjustified higher (or lower) pricing is done for subsequent years.
9. The bidder needs to account for all Out of Pocket expenses due to Boarding, Lodging and other related items.
10. VSCDL reserves the right to do market survey for bid prices offered and negotiate with the bidder if their prices are higher than the ones discovered at that point of time.
11. For Commercial Bid calculation purpose, each of the line items in the above schedule shall be considered for specified units. However the actual quantity of the order could be different than the numbers given in these Schedule, and would be based on actual requirements.
12. All the manpower/resources considered is for yearly deployment period. Bidder is expected to factor the necessary leaves of the resources to ensure continuous availability on all working days of VSCDL (as per VSCDL Calendar) within the man-power cost quoted. However, the manpower should be available to carry out scope of work items, to meet the SLA requirements.
13. The manpower cost shall be considered for Commercial Bid evaluation. However, the same cost cannot guaranteed for actual deployment as the requirements may change (decreased or increased) during subsequent years.
14. The bidder who has the lowest Commercial will be selected as the successful bidder and may be awarded the Contract.
15. If the commercials received from the bidders exceeds beyond 10% of the total project cost estimated by VSCDL, the bids will be rejected.

Summary of Cost Components

Schedule S: Summary of All Cost Components

Sr.	Description	Total Amount without Taxes	Total Taxes Amount	Total Amount with Taxes
		S1	S2	S=S1+S2
Phase I				
I1	CAPEX : A - Cyber Security Equipment			
I2	CAPEX : B - Implementation and Training			
I3	OPEX : C - AMC of Cyber Security Equipment			
I4	OPEX : D – Manpower			
	Phase I Subtotal (A+B+C+D)			
Phase II				
II1	CAPEX : E - Cyber Security Equipment			
II2	CAPEX : F - Implementation and Training			
II3	OPEX : G - AMC of Cyber Security Equipment			
	Phase II Subtotal (E+F+G)			
S=Grand Total (Phase I + Phase II) in Rs.				

Note: Above value (S) will be used for Commercial Bid evaluation (L1 position) purpose.

You are required to input (punch in) all-inclusive item rates on (n)procure, i.e. prices inclusive of all taxes and levies

Schedule A: Cyber Security Equipment (Phase I)

Schedule A									
Sr.	Item	UOM	Qty.	Basic Rate	Total Cost (Excluding Taxes)	Taxes		Total Taxes	Total Amount with Taxes
			Q	A	D= A*Q	Rate	Amount	G = E+F	T= D+G
1.	NG Firewall (External) (1+1 in HA mode)	Number	2						
2.	Web Application Firewall solution	Number	1						
3.	Additional AV Licenses for Servers	Number	250						
4.	Additional AV Licenses for Desktops	Number	500						
5.	SIEM solution	Lot	1						
6.	PIM Solution	Lot	1						
7.	Integration with existing HSM	Lot	1						
8.	Implementation cost for Phase I Security Components								
9.	Any Other Cost (please specify in tech bid)	L/S	1						
Total Cost (INR) for This schedule									

** Above cost shall include Solution sizing, supply, installation, testing, commissioning and integration (CCC at Badamdi Baug) of the above components, with ONE year Comprehensive Hardware and Software warranty post Go-live.*

(#) Please provide complete details and BoQ with make and model, of such “Any other item” along with Technical Proposal.

Schedule B: Implementation Cost (Phase I)

Schedule B									
Sr.	Item	UOM	Qty.	Basic Rate	Total Cost (Excluding Taxes)	Taxes		Total Taxes	Total Amount with Taxes
			Q	A	D= A*Q	Rate	Amount	G = E+F	T= D+G
1.	IT Infrastructure and Security Review	Lot	1						

2.	IT Security Policy Preparation and Implementation of Security Governance Framework	Lot	1						
3.	Training	Lot	1						
4.	Any Other Cost for Phase I	L/S							
	Total – Schedule B (in INR)								

Schedule C: AMC and Technical Support for O &M period (Phase I)**Schedule C**

#	Components	UoM	Quantity	Total for Year 1	Total for Year 2	Total for Year 3	Total for Year 4	Total for 5 years
1	NG Firewall (External) (1+1 in HA mode)	Number	2					
2	Web Application Firewall solution	Lot	1					
3	Additional AV Licenses for Servers	Number	250					
4	Additional AV Licenses for Desktops	Number	500					
5	SIEM solution	Lot	1					
6	PIM Solution	Lot	1					
7	VAPT + Threat Intelligence periodic test/review	Lot	1					
8	Any Other Cost (Please specify in tech bid)	L/S	1					
	Total price (INR) for this schedule (#) (all prices are with taxes)							

(#) AMC cost for Hardware items would start from 2nd year, as Capital cost asked is with 1 year warranty and AMC

Schedule D: CSOC Manpower Cost for O&M period (Phase I)**Schedule D**

#	Components	UoM	Quantity	Total for Year 1	Total for Year 2	Total for Year 3	Total for Year 4	Total for 5 years

RFP for Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)

1	SOC Lead -cum – CISO	On site resource	1					
2	L3 - Enterprise Application Security Professional	On site resource	1					
3	L2 - Data Protection Analysts IoT / Endpoint Security	On site resource	1					
4	L1 - IT Analysts / Auditors	On site resource	1					
5	O&M Staff for managing cyber security components	On site resource	As per O&M requirements for managing Security Components					
6	Any Other Cost (Please specify in tech bid)	L/S						
	Total price (INR) for this schedule (all prices are with taxes)							

Schedule E: Cyber Security Equipment (Phase II)

Schedule E									
Sr.	Item	UOM	Qty.	Basic Rate	Total Cost (Excluding Taxes)	Taxes		Total Taxes	Total Amount with Taxes
						Rate	Amount		
			Q	A	D= A*Q	E	F	G = E+F	T= D+G
1.	Server Security (HIPS) (For servers)	Lot	1						
2.	DLP Solution (End point, Web, Network, File Share)	Lot	1						
3.	Anti APT Solution	Lot	1						
4.	NAC (Network Access Control) Solution	Lot	1						
5.	2 Factor Authentication	Lot	1						

6.	Any Other Cost (Please specify in tech bid)	L/S	1						
	Total Cost for This Schedule (in INR)								

*** Above cost shall include hardware sizing, supply, installation, testing, commissioning and integration (CCC at Badamdi Baug) of the above components, with ONE Hardware and Software warranty post Go-live.**

(#) Please provide complete details and BoQ with make and model, of such “Any other item” along with Technical Proposal.

Schedule F: Implementation Cost (Phase II)

Schedule F									
Sr.	Item	UOM	Qty	Basic Rate	Total Cost (Excluding Taxes)	Taxes		Total Taxes	Total Amount with Taxes
			Q	A	D= A*Q	Rate	Amount	G = E+F	T= D+G
1.	Implementation cost for Phase II	Lot	1						
2.	Training Costs for Phase-II	Lot	1						
3.	Any Other Cost for Phase II	L/S	1						
	Total for this schedule (in INR)								

Schedule G: AMC and Technical Support for O &M period (Phase II)

Schedule G								
#	Components	UoM	Quantity	Total for Year 1	Total for Year 2	Total for Year 3	Total for Year 4	Total for 5 years
1	Server Security (HIPS) (For servers)	Lot	1					
2	DLP Solution (End point, Web, Network, File Share)	Lot	1					
3	Anti APT Solution	Lot	1					
4	NAC (Network Access Control) Solution	Lot	1					
5	2 Factor Authentication	Lot	1					
6	O&M Support Staff for Phase-II Components	No.	As per O&M requirements for managing					

RFP for Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)

			Security Components					
7	Cyber Liability insurance premium (yearly)	Lot	1					
8	Any Other Cost (Please specify in tech bid)	L/s	1					
	Total price (INR) for this schedule(#) (all prices are with taxes)							

(#) AMC cost for Hardware items would start from 2nd year, as Capital cost asked is with 1 year Comprehensive warranty

13 Annexure V – List of IT Projects

The following projects would in included for the assignment under this RFP.

#	Project Name	Description	Primary Site	ILL at Primary	P2P	Secondary Site (DR)	ILL at DR	Existing Security Infrastructure	Major Applications
1	ICCC Projects	Integrated Command and Control Center, OFC Network, A number of IoT devices Other sub-projects under ICCC Project	CCC, Badamadi Baug, Vadodara	100 Mbps Jio 50 Mbps BSNL	50 Mbps Tata 50 Mbps Vodafone	ESDS Nashik	50 Mbps by cloud service provider	Firewalls + IPS (Fortigate FG800D),	IBM IOC Videonetics Traffview (CMS) etc
2	Public Wifi and iPoles	Approximate 450 Wifi hotspots, OFC Network (in PPP Mode).	CCC, Badamadi Baug, Vadodara	200 Mbps Vodafone	NA (OFC Network to all Wifi APs)	NA	NA	Fortigate 500E	Cisco Wifi Controller, Vodafone BSS/OSS for wifi
3	ERP (eGovernance for VMC)	SAP and non-SAP based eGovernance systems for VSCDL (approx. 350 users / desktops. This system in under implementation.	CCC, Badamadi Baug, Vadodara	Uses ICCC ILL and VMC ILL	BSNL P2P to all wards, OFC WAN	NA	NA	nCipher nShield Connect	SAP ERP, Custom developed non-core applications in Dot Net
4	Intelligent Transit Management System	GPS on 150 City Buses, PIS displays on 125 Bus stops	CCC, Badamadi Baug, Vadodara	50 Mbps Tata ILL	NA	NA	NA	Sophos XG310	AryaOmnitalk ITMS Applications
5	My Vadodara Mobile App	Mobile App for citizen (on IOS and Android Platform)	Third Party	Microsoft	Cloud provider link	NA	NA	Cloud based security from Azure	Custom programming

RFP for Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)

#	Project Name	Description	Primary Site	ILL at Primary	P2P	Secondary Site (DR)	ILL at DR	Existing Security Infrastructure	Major Applications
				Azure Cloud (Mumbai)					
6	Health Management Information System (HMIS)	HMIS system on cloud for around 40 Urban primary Health Canters	Microsoft Azure Cloud	Jio 8 Mbps	Jio MPLS to all UPHC	Microsoft Azure Cloud (Chennai)	Jio 8 Mbps	Firewall/UTM on cloud	HMIS from Manorama, Custom Applications
7	SCADA	SCADA system for (a) Water and (b) STP	CCC, Badamadi Baug, Vadodara	Uses ICCC ILL	Sim Based Network	NA	NA	NA	Siemens Application
8	On-Surface GIS	A GIS system with 70+ layers of geographical and other information about VSCDL assets above and below ground	CCC, Badamadi Baug, Vadodara	Uses ICCC ILL	NA	NA	NA	NA	QGIS GeoServer
9	Automatic Land Encroachment Prevention System	Other IT projects of Vadodara Smart City that will come in near future	CCC, Badamadi Baug, Vadodara	Uses ICCC ILL	NA	NA	NA	NA	Internet based portal, custom dev app for Plot alerts
10	ICT upgradation of Fire stations	IT Enablement of 6 firestations and 30 Fire trucks, Dispatch System	CCC, Badamadi Baug, Vadodara	Uses ICCC ILL	NA	NA	NA	NA	AryaOmnitalk Fleet
11	EGovernance Systems of VMC and VMC Website	Existing running eGovernance Systems of VMC such as Property Tax, Birth and Death	Server Room at Khanderrao Market HQ	50 Mbps BSNL ILL at Server Room at	BSNL P2P links to all Wards	NA	NA	NA	Custom Developed Apps and Web Portal

RFP for Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)

#	Project Name	Description	Primary Site	ILL at Primary	P2P	Secondary Site (DR)	ILL at DR	Existing Security Infrastructure	Major Applications
		registration, Licenses etc. on VMC Website		Khanderrao Market HQ					

Indicative sizing requirement:

S.No.	Devices	Approximate Qty.
1.	Number of Applications to be integrated with cyber security solutions	40
2.	Number of devices for Vulnerability Assessment and Penetration Testing	1500 (Assume 1 IP address for each device)
3.	Number of devices for Data Loss Prevision end points (Desktop + Workstations+ tablets)	600
4	Number of users requiring PIM	200
5.	Number of users requiring two factor authentications	300

Note:

1. Please note that the above table gives approximate quantity ONLY. The bidder is required to carry out design and sizing of the solution as per best practices to achieve most economical and efficient solution. The project list is given above, bidders are requested to size and calculate license requirement for each of the cyber security solution components.
2. The bidder is expected to take the details of the inventory at the time of project implementation.
3. The Selected bidder will assist the VSCDL in incorporating the newer hardware devices with all the tools

14 Annexure VI- Common guidelines/requirements regarding compliance of equipment

Other/General Criteria

1. The specifications mentioned for various IT / Non-IT components are indicative requirements and should be treated for benchmarking purpose only. SIs are required to undertake their own requirement analysis and may propose higher specifications that are better suited to the requirements.
2. Any manufacturer and product name mentioned in the Tender should not be treated as a recommendation of the manufacturer / product, unless specifically mentioned so.
3. None of the IT / Non-IT equipment's proposed by the SI should be End of Life product. It is essential that the technical proposal is accompanied by the OEM certificate in the format given in this Tender, where-in the OEM will certify that the product is not end of life product & shall support for at least 4 years from the date of Bid Submission.
4. All IT Components should support IPv4 and IPv6
5. Technical Bid should be accompanied by OEM's product brochure / datasheet. SIs should provide complete Make, model, part numbers and sub-part numbers for all equipment/software quoted, in the Technical Bid, as per section 8.1
6. SIs should ensure complete warranty and support for all equipment from OEMs. All the back-to-back service agreements should be submitted along with the Technical Bid.
7. All equipment, parts should be original and new.
8. The user interface of the system should be a user friendly Graphical User Interface (GUI).
9. Critical core components of the system should not have any requirements to have proprietary platforms and should conform to open standards.

10. For custom made modules, industry standards and norms should be adhered to for coding during application development to make debugging and maintenance easier. Object oriented programming methodology must be followed to facilitate sharing, componentizing and multiple-use of standard code. Before hosting the application, it shall be subjected to application security audit (by any of the CERTIN empanelled vendors) to ensure that the application is free from any vulnerability; and approved by the VSCDL.
11. All the Clients Machines / Servers shall support static assigned IP addresses or shall obtain IP addresses from a DNS/DHCP server.
12. The Successful SI should also propose the specifications of any additional servers / other equipment/hardware/software, if required for the system.
13. The indicative architecture of the system is given in this tender. The Successful SI must provide the architecture of the solution it is proposing.
14. The system servers and software applications might hosted in existing Data Centres (CCC, Badamdi Baug) or client will take the final decision (for selection of location)for hosting the server for this project.
15. The Servers provided should meet industry standard performance parameters (such as CPU Utilisation of 70 percent). In case any non-standard computing environment is proposed, detail clarification needs to be provided in form of supporting documents, to confirm (a) how the sizing has been arrived at and (b) how SLAs would be met.
16. SI is required to ensure that there is no choking point / bottleneck anywhere in the system (end-to-end) and enforce performance and adherence to SLAs. SLA reports must be submitted as specified in the Bid without fail.
17. All the hardware and software supplied should be from the reputed Original Equipment Manufacturers (OEMs). VSCDL reserves the right to ask replacement of any hardware / software if it is not from a reputed brand and conforms to all the requirements specified in the tender documents.
18. Service Provider shall place orders on various OEMs directly and not through any sub-contractor / partner. All licenses should be in the name of the VSCDL.

15 Annexure VII: Format for Performance Bank Guarantee

<<To be printed on INR 300/- Stamp Paper>>

IN CONSIDERATION OF _____ through _____
Vadodara Smart City Development Corporation (VSCDL) for “**Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)**” (hereinafter referred to as the “said work”) on the terms and conditions of the AGREEMENT dated the _____ day of _____ 201X executed between VSCDL on the one part and the Company (_____) on the other part (hereinafter referred to as “the said AGREEMENT”) and on the terms and conditions specified in the Contract, Form of Offer and Form of Acceptance of Offer, true and complete copies of the offer submitted by the Company, the said Acceptance of Offer and the said AGREEMENT are annexed hereto.

The Company has agreed to furnish VSCDL in Guarantee of the Nationalized Bank for the sum of INR _____ (Rupees _____ only) only which shall be the Security Deposit for the due performance of the terms covenants and conditions of the said AGREEMENT. We _____ Bank registered in India under Act and having one of our local Head Office at _____ do hereby guarantee to VSCDL in _____ Department.

- i. Due performance and observances by the Company of the terms covenants and conditions on the part of the Company contained in the said AGREEMENT, AND
- ii. Due and punctual payment by the Company to VSCDL of all sum of money, losses, damages, costs, charges, penalties and expenses that may become due or payable to VSCDL by or from the Company by reason of or in consequence of any breach, non-performance or default on the part of the Company of the terms covenants and conditions under or in respect of the said AGREEMENT.

AND FOR THE consideration aforesaid, we do hereby undertake to pay to VSCDL on demand without delay demur the said sum of INR _____ (Rupees _____ only) together with interest thereon at the rate prescribed under _____ from the date of demand till payment or such lesser sum, as may be demanded by VSCDL from us as and by way of indemnity on account of any loss or damage caused to or suffered by VSCDL by reason of any breach, non-performance or default by the Company of the terms, covenants and conditions contained in the said AGREEMENT or in the due and punctual payment of the moneys payable by the Company to VSCDL thereunder and notwithstanding any dispute or disputes raised by the Company in any suit or proceeding filed before the Court relating thereto our liability hereunder being absolute and unequivocal and irrevocable AND WE do hereby agree that:

- a) The guarantee herein contained shall remain in full force and effect during the subsistence of the said AGREEMENT and that the same will continue to be enforceable till all the claims of VSCDL are fully paid under or by virtue of the said AGREEMENT and its claims satisfied or discharged and till VSCDL certifies that the terms and conditions of the said AGREEMENT have fully and properly carried out by the Company.
- b) We shall not be discharged or released from liability under this Guarantee by reason of
 - a. any change in the Constitution of the Bank or
 - b. any arrangement entered into between VSCDL and the Company with or without our consent;
 - c. any forbearance or indulgence shown to the Company,
 - d. any variation in the terms, covenants or conditions contained in the said AGREEMENT;
 - e. any time given to the Company, OR
 - f. Any other conditions or circumstances under which in a law a surety would be discharged.
- c) Our liability hereunder shall be joint and several with that of the Company as if we were the principal debtors in respect of the said sum INR _____ (Rupees _____ only).
- d) We shall not revoke this guarantee during its currency except with the previous consent of VSCDL in _____ Department in writing;

- e) Provided always that notwithstanding anything herein contained our liabilities under this guarantee shall be limited to the sum of INR _____ (Rupees _____ only) and shall remain in force until VSCDL certifies that the terms and conditions of the said AGREEMENT have been fully and properly carried out by the Company.
- f) Bank hereby agrees and covenants that if at any stage default is made in payment of any instalment or any portion thereof due to VSCDL under the said AGREEMENT or if the Company fails to perform the said AGREEMENT or default shall be made in fulfilling any of the terms and conditions contained in the said AGREEMENT by the Company, the Bank shall pay to VSCDL demand without any demur, such sum as may be demanded, not exceeding INR _____ (Rupees _____ only) and that the Bank will indemnify and keep VSCDL indemnified against all the losses pursuant to the said AGREEMENT and default on the part of the Company. The decision of VSCDL that the default has been committed by the Company shall be conclusive and final and shall be binding on the Bank/Guarantor. Similarly, the decision of VSCDL as regards the Agreement due and payable by the Company shall be final and conclusive and binding on the Bank /Guarantor.
- g) VSCDL shall have the fullest liberty and the Bank hereby gives its consent without any way affecting this guarantee and discharging the Bank/Guarantor from its liability hereunder, to vary or modify the said AGREEMENT or any terms thereof or grant any extension of time or any facility or indulgence to the Company and Guarantee shall not be released by reason of any time facility or indulgence being given to the Company or any forbearance act or omission on the part of VSCDL or by any other matter or think whatsoever which under the law, relating to sureties so releasing the guarantor and the Guarantor hereby waives all suretyship and other rights which it might otherwise be entitled to enforce.
- h) That the absence of powers on the part of the Company or VSCDL to enter into or execute the said AGREEMENT or any irregularity in the exercise of such power or invalidity of the said AGREEMENT for any reason whatsoever shall not affect the liability of the Guarantor/Bank and binding on the bank notwithstanding any abnormality or irregularity,
- i) The Guarantor agrees and declares that for enforcing this Guarantee by _____ against it, the Courts at Vadodara only shall have exclusive jurisdiction and the Guarantor hereby submits to the same.

1. _____
2. _____

Being respectively the Director of the Company, who in token thereof, has hereto set his respective hands in the presence of:

1. _____
2. _____

16 Annexure VIII: Master Service Agreement

<<To be printed on Stamp Paper of Rs 300>>

This **AGREEMENT** is made at _____, Vadodara, Gujarat, on this ____ day of _____, _____,
BETWEEN

-----, hereinafter referred to as "**Client**", or "**VSCDL**" (which expression unless repugnant to the context therein shall include its administrator and permitted assignees) of the **FIRST PART**;

AND

-----, a company registered under the Companies Act, 1956, having its registered office at ---
-----, hereinafter referred to as "**Systems Integrator**" or "**SI**" or "**Vendor**", (which expression unless repugnant to the context therein, shall include its successors, administrators, executors and permitted assignees), of the **SECOND PART**.

The VSCDL and the System Integrator shall be collectively referred to as the "Parties".

Whereas VSCDL has envisaged to implement Cyber Security IN VADODARA CITY

And whereas VSCDL published the RFP to seek services of a reputed IT firm as a Service Provider for Design, Development, Implementation and Maintenance of Cyber Security IN VADODARA CITY

And whereas M/s. ----- has submitted its proposal for "**Selection of Service Provider for Implementation of Cyber Security Solutions and CSOC for VSCDL (Second Attempt)**";

AND whereas VSCDL has selected M/s..... as successful bidder and issued Letter of Intent dated to the successful bidder who in turn signed and returned the same as a token of acceptance of Letter of Intent.

And whereas VSCDL and M/s. ----- have decided to enter into this Agreement on the terms and conditions stipulated hereinafter.

NOW, THEREFORE, in consideration of the premises covenants and promises contained herein and other good and valuable considerations, the receipt and adequacy of which is hereby acknowledged, the parties intending to be bound legally, IT IS HEREBY AGREED between the Parties as follows:

1. Definitions

In this Agreement, the following terms shall be interpreted as indicated, -

- (a) "VSCDL" means Vadodara Smart City Development Limited
- (b) "Contract" means this Agreement entered into between VSCDL and the Systems Integrator including all attachments and annexure thereto and all documents incorporated by reference therein;
- (c) "Systems Integrator" means M/s. ----- interchangeably referred to as "SI" in the contract; and
- (d) "RFP" means the Tender Published by VSCDL (Ref. No. -----) and the subsequent Corrigenda/ Clarifications issued.
- (e) "Go Live or successful completion of implementation of the project" date means the 16th day after the date on which the proposed project stream becomes operational after successful conclusion of all acceptance tests to the satisfaction of VSCDL.
- (f) "Deliverable" means any action / output generated by the SI while discharging their contractual obligations. This would include information and all the other services rendered as per the scope of work and as per the SLAs.

- (g) "Assets" refer to all the hardware / software / furniture / data / documentation / manuals / catalogues / brochures / or any other material procured, created, or utilised by the SI for the Vadodara City 'Cyber Security' Project.
- (h) "Services" means any work executed or service provided as a party of this contract or which is in scope of work for the System Integrator as a part of this contract.

2. Interpretation

The documents forming this Agreement are to be taken as mutually explanatory of one another. The following order shall govern the priority of documents constituting this Agreement, in the event of a conflict between various documents, the documents shall have priority in the following order:

- Clarification & Corrigendum Documents published by VSCDL subsequent to the RFP for this work (hereby annexed as **Annexure**)
- RFP Document of VSCDL for this work (hereby annexed as **Annexure**) subject to the deviation expressly mentioned in the deviation sheet submitted herein
- this Agreement;
- Scope of Services for the Systems Integrator (hereby annexed as **Annexure**)
- Detail Commercial proposal of the Systems Integrator accepted by VSCDL (hereby annexed as **Annexure**)
- SLA to be adhered by the Systems Integrator (hereby annexed as **Annexure**)
- LoI issued by the VSCDL to the successful bidder (hereby annexed as **Annexure**); and
- Successful bidder's "Technical Proposal" and "Commercial Proposal" submitted in response to the RFP (hereby annexed as **Annexure**)

Any word or expression used in this Agreement shall, unless otherwise defined or construed in this Agreement, bear its ordinary English meaning and, for these purposes, the General Clauses Act, 1897 shall not apply

The rule of construction, if any, that a contract should be interpreted against the Party responsible for the drafting and preparation thereof, shall not apply.

3. Term of the Agreement

The term of this Agreement shall constitute implementation phase and a period of 5 years from the date of Go-Live of all project components.

In the event of implementation period getting extended beyond implementation timelines, for reasons not attributable to the Systems Integrator, VSCDL reserves the right to extend the term of the Agreement by corresponding period to allow validity of contract for 5 years from the date of successful completion of implementation of all the project components. (Note: Delay caused due to any reason not in control of the SI would not be attributed to the project period.)

VSCDL also reserves the right to extend the contract at its sole discretion for additional duration, beyond the 5 years of post-implementation period. Terms and conditions of such an extension shall be prepared by VSCDL and finalized in mutual discussion with the SI.

4. Work Completion Timelines and Payment Terms

Project delivery/work completion milestones and payment milestones shall be as per Section 9 of Volume 1. Milestones shall be from the date of work order.

5. Scope Extension

VSCDL reserves right to extend the scope of services for the price and timelines, as per terms and condition of the RFP as given in RFP, in accordance with the change management procedure as given in Annexure XX of this volume after a notice to the successful bidder. The SLAs applicable to this Contract shall be applicable for the additional items too..

6. Service Level Agreement (SLA)

Systems Integrator shall, at all times, maintain a very professional approach in the project implementation and its operations, and is expected to match the expectations of the service levels given in Annexure XX of this agreement. Any non-adherence to the SLAs would lead to the penalty, to be calculated as per the details given in Annexure XX to this agreement.

7. Use and Acquisition of Assets during the Term

Systems Integrator hereby agrees that it shall:

- Take all reasonable and proper care of the entire hardware & software, network or any other information technology infrastructure components used for the project & other facilities leased/owned by the Systems Integrator exclusively in terms of the delivery of the services as per this Agreement (hereinafter the “Assets” which include all the hardware/software/furniture/data/documentations/manuals/catalogues/brochures/or any other material procured, created or utilized by the SI or the VSCDL for the Vadodara CYBER SECURITY Project in proportion to their use and control of such Assets which will include all upgrades/enhancements & improvements to meet the needs of the project arising from time to time;

The Parties hereby agree that the Assets would be owned by the VSCDL however, the Systems Integrator would be custodian of the same during the entire contract period and would take care of all wear-tear, insurance, theft etc. so that the SLAs are not affected. If any upgrade on project equipment is required beyond the scope of the RFP, the parties shall enter into a change request, which shall be honoured by both the sides.

- Maintain sufficient spare inventory at all times, for all items of importance;
- Keep all the tangible Assets in good and serviceable condition (reasonable wear & tear excepted) &/or the intangible Assets suitably upgraded subject to the relevant standards as stated in of the RFP to meet the SLAs mentioned in the contract & during the entire term of the Agreement.
- Ensure that any instructions or manuals supplied by the manufacturer of the Assets for use of Assets and which are provided to the Systems Integrator will be followed by the Systems Integrator & any person who will be responsible for the use of the Asset;
- Take such steps as may be recommended by the manufacturer of the Assets and notified to the Service Provider or as may be necessary to use the Assets in a safe manner;
- Provide a well-prepared documentation for users in the manual, a clear plan for training, education & hand holding the users and shall form part of hand holding phase until bringing up the users to use software solution with speed & efficiency;
- To the extent that the Assets are under the control of the Systems Integrator , keep the Assets suitably housed and in conformity with any statutory requirements from time to time applicable to them;
- Provide and facilitate access to VSCDL or its nominated agencies & any persons duly authorized by him/her to enter any land or premises on which the Assets are for the time being sited so as to inspect the same, subject to any reasonable requirements;
- Not, knowingly or negligently use or permit any of the Assets to be used in contravention of any statutory provisions or regulation or in any way contrary to law;
- Use the Assets exclusively for the purpose of providing the Services as defined in the contract;
- Use the Assets only in accordance with the terms hereof & those contained in the SLAs;

- Maintain standard forms of comprehensive insurance including liability insurance, system and facility insurance & any other insurance for the Assets, data, software, etc. in the joint names of VSCDL & the Systems Integrator, where SI shall be designated as the 'loss payee' in such insurance policies; SI shall be liable to pay premium for the insurance policy & shall ensure that each & every policy shall keep updated from time to time.
- Ensure the integration of the software with hardware to be installed and the current Assets in order to ensure the smooth operations of the entire solution architecture to provide efficient services to VSCDL of this project in an efficient and speedy manner; &
- Obtain a sign off from VSCDL or its nominated agencies at each stage as is essential to close each of the above considerations.

Ownership of the Assets shall vest with VSCDL on Go Live of the project. Ownership of any asset, created during the contractual period after go Live, shall also vest with VSCDL upon creation of such asset. Service Provider shall not use VSCDL data to provide services for the benefit of any third party, as a service bureau or in any other manner. Six months prior to the expiry of the contract (of the respective work streams), there shall be joint inspection by a team of VSCDL and SI to assess the damages to the assets, if any. If damage to the assets is found unacceptable to the VSCDL, then corresponding penalty/liquidated damages shall be recovered from SI from the fees payable. The SI at all times shall ensure that it takes sufficient care of all the Assets, as if it were the property of the SI.

8. Security and Safety

- It shall be the duty of the Systems Integrator to follow Good Industry Practice at all times and maintain the security and safety of all personnel, including any third-party contractors, agents, individuals proprietors, etc., who are working towards the objectives of this Agreement. The SI shall also take reasonable care and safety to ensure that all the Assets, including all intangible assets, data, information, trade know-hows, are protected and secured at all times.
- The Systems Integrator will comply with the directions issued from time to time by VSCDL and the standards related to the security and safety in so far as it applies to the provision of the Services.
- Systems Integrator shall also comply with the VSCDL Project's information technology security and standard policies in force from time to time as applicable.
- Systems Integrator shall, on its own accord, use reasonable endeavours to report forthwith in writing to all the partners / contractors about the civil and criminal liabilities accruing due to by unauthorized access (including unauthorized persons who are employees of any third party) or interference with VSCDL's data, facilities or Confidential Information.
- The Systems Integrator shall upon reasonable request by VSCDL or his/her nominee(s) participate in regular meetings when safety and information technology security matters are reviewed.
- Systems Integrator and its partners/sub-contractors shall promptly report in writing to each other and VSCDL any act or omission which they are aware that could have an adverse effect on the proper conduct of safety and information technology security at VSCDL's Facilities.
- In case of any breach of safety or security due to the negligence of the System Integrator or its partners or sub-contractors, it shall be the duty of the System Integrator to immediately take reasonable steps to prevent any further breach of safety or security and the System Integrator shall immediately make good the loss and VSCDL shall examine the same and may impose reasonable penalty on the System Integrator.
-

9. Insurance

The Goods supplied under this Agreement shall be comprehensively insured by SI at his own cost, against any loss or damage, for the entire period of the contract. SI must have and maintain for the Agreement Period, valid and enforceable insurance coverage for all its activities, products, services, including but not limited to:

- public liability;
- either professional indemnity or errors and omissions;
- product liability;
- workers' compensation as required by law
- fire and transit insurance

2. SI shall submit to VSCDL, documentary evidence issued by the insurance company, indicating that such insurance has been taken.

3. SI shall bear all the statutory levies like customs, insurance, freight, etc. applicable on the goods and the charges like transportation charges, octroi, etc. that may be applicable till the goods are delivered at the respective sites of installation.

4. SI shall take and maintain at its own cost, on terms and conditions approved by VSCDL, insurance against the risks, and for the coverage's, for employer's liability and workers' compensation insurance in respect of the Personnel of the Company, in accordance with the relevant provisions of the applicable laws, as well as, with respect to such personnel, any such life, health, accident, travel or other insurance as may be appropriate.

5. At the request of VSCDL, SI shall provide evidence indicating that such insurance has been taken - and maintained and that the current premiums have been paid.

6. At any of point during the subsistence of this Agreementt, if the SI has to claim any amount from the insurance providers, SI shall submit all the necessary documentary evidence and claims. The VSCDL shall assist the SI by providing additional supporting documents, if any, required by SI for claiming insurance. The SI shall file the claim with the insurance company, and VSCDL and the SI shall both co-operate during the insurance investigation process and shall allow all the insurance agents, surveyors, or officials to visit the necessary sites and review the claims and other relevant documents. The SI and VSCDL shall jointly ensure that the necessary documents required for claiming the insurance are available and supplied to the insurance company within the time frame mentioned in the insurance policy. Any claim, reimbursement, payment, compensation, amount, in part or whole, received during or after insurance process shall be remitted to the account of the SI.

10. Indemnity

The Systems Integrator agrees to indemnify and hold harmless VSCDL, its officers, employees and agents(each a "Indemnified Party") promptly upon demand at any time and from time to time, from and against any and all losses , claims, damages, liabilities, costs (including reasonable attorney's fees and disbursements) and expenses (collectively, "Losses") to which the Indemnified Party may become subject, in so far as such losses directly arise out of, in any way relate to, or result from

- i. Any misstatement or any breach of any representation or warranty made by the Service Provider or
- ii. The failure by the Service Provider to fulfil any covenant or condition contained in this Agreement, including without limitation the breach of any terms and conditions of this Agreement by any employee or agent of the Service Provider.
- iii. All losses or damages arising from claims by third Parties that any Deliverable (or the access, use or other rights thereto), created Service Provider pursuant to this Agreement, or any equipment, software, information, methods of operation or other intellectual property created by Service Provider or sub-contractors pursuant to this Agreement, or the SLAs (I) infringes a copyright, trade mark, trade design enforceable in India, (II) infringes a patent issued in India, or (III) constitutes misappropriation or

unlawful disclosure or use of another Party's trade secrets under the laws of India (collectively, "Infringement Claims"); provided, however, that this will not apply to any Deliverable (or the access, use or other rights thereto) created by (A) "Implementation of project by itself or through other persons other than Service Provider or its sub-contractors; (B) Third Parties (i.e., other than Service Provider or sub-contractors) at the direction of VSCDL, or

- iv. any compensation / claim, including all legal, administrative, arbitration fees, to be paid to any third party arising out of proceedings against VSCDL due to any act, deed or omission by the Service Provider or
- v. Any claim, suit, petition, notice filed/issued by a workman, employee, sub-contractor, partners, vendors, Service Provides, engaged by the SI for carrying out work related to this Agreement.

or the avoidance of doubt, indemnification of Losses pursuant to this section shall be made in an amount or amounts sufficient to restore each of the Indemnified Party to the financial position it would have been in had the losses not occurred Any payment made under this Agreement to an indemnity or claim for breach of any provision of this Agreement shall include applicable taxes.

11. Third Party Claims

- a. Subject to Sub-clause (b) below, the Systems Integrator agrees to Indemnify and hold harmless VSCDL, its officers, employees and agents, from and against all losses, claims litigation and damages on account of bodily injury, death or damage to tangible personal property arising in favour or any person, corporation or other entity) attributable to the Indemnifying Party's performance or non-performance under this Agreement or the SLAs.
- b. The indemnities set out in Sub-clause (a) above shall be subject to the following conditions:
 - i. The Indemnified Party, as promptly as practicable, informs the Indemnifying Party in writing of the claim or proceedings and provides all relevant evidence, documentary or otherwise;
 - ii. The Indemnified Party shall, at the cost and expenses of the Indemnifying Party, give the Indemnifying Party all reasonable assistance in the defence of such claim including reasonable access to all relevant information, documentation and personnel. The Indemnifying Party shall bear cost and expenses and fees of the Attorney on behalf of the Indemnified Party in the litigation, claim, notice, or other similar charges.
 - iii. If the Indemnifying Party does not assume full control over the defence of a claim as provided in this Article, the Indemnified Party may participate in such defence at its sole cost and expense, and the Indemnified Party will have the right to defend the claim in such manner as it may deem appropriate, and the cost and expense of the Indemnified Party will be borne and paid by the Indemnifying Party.
 - iv. The Indemnified Party shall not prejudice, pay or accept any proceedings or claim, or compromise any proceedings or claim, without the written information to the Indemnifying Party;
 - v. Systems Integrator hereby indemnify and hold indemnified the VSCDL harmless from & against any & all damages, losses, liabilities, expenses including legal fees & cost of litigation in connection with any action, claim, suit, proceedings as if result of claim made by the third party directly or indirectly arising out of or in connection with this agreement.
 - vi. All settlements of claims subject to indemnification under this Article will: (a) be entered into only with the consent of the Indemnified Party, which consent will not be unreasonably withheld & include an unconditional release to the Indemnified Party from the claimant for all liability in

respect of such claim; and (b) include any appropriate confidentiality agreement prohibiting disclosure of the terms of such settlement;

- vii. The Indemnified Party shall take steps that the Indemnifying Party may reasonably require to mitigate or reduce its loss as a result of such a claim or proceedings;
- viii. In the event that the Indemnifying Party is obligated to indemnify an Indemnified Party pursuant to this Article, the Indemnifying Party will, upon payment of such indemnity in full, be subrogated to all rights & defences of the Indemnified Party with respect to the claims to which such indemnification relates;
- ix. In the event that the Indemnifying Party is obligated to indemnify the Indemnified Party pursuant to this Article, the Indemnified Party will be entitled to invoke the Performance Bank Guarantee, if such indemnity is not paid, either in full or in part, and on the invocation of the Performance Bank Guarantee, the Indemnifying Party shall be subrogated to all rights & defences of the Indemnified Party with respect to the claims to which such indemnification relates.

12. Publicity

Any publicity by the SI in which the name, logo, of VSCDL is to be used or if any attribution is to be made VSCDL, should be done only after obtaining explicit written permission of the CEO, VSCDL.

13. Warranties

- a. The Systems Integrator warrants and represents to VSCDL that:
 - i. It has full capacity, permissions, approvals, authority and is legally competent to enter into and to perform its obligations under this Agreement;
 - ii. This Agreement is executed by a duly authorized representative of the Systems Integrator;
 - iii. It shall discharge its obligations under this Agreement with due skill, care and diligence so as to comply with the Service Level Agreements.
- b. In the case of the SLAs, the Systems Integrator warrants and represents to VSCDL, that:
 - the Systems Integrator has full capacity and authority and all necessary approvals to enter into and perform its obligations under the SLAs and to provide the Services;
 - The SLAs have been executed by a duly authorized representative of the Systems Integrator;
 - The Systems Integrator is experienced in managing and providing works similar to the Services and that it will perform the Services with all due skill, care and diligence so as to comply with service level agreement;
 - The Services will be provided and rendered by appropriately qualified, trained and experienced personnel as mentioned in the RFP;
 - Systems Integrator has and will have all necessary licenses, approvals, consents of third Parties free from any encumbrances and all necessary technology, hardware and software to enable it to provide the Services;
 - The Services will be supplied in conformance with all laws, enactments, orders and regulations applicable from time to time;
 - Systems Integrator will warrant that the goods supplied under the contract are new, unused, of the most recent higher version /models and incorporate all recent improvements in design and

materials unless provided otherwise in the contract. The Service Provider further warrants that the goods supplied under this contract shall have no defects arising from design, materials or workmanship.

- The overall system design shall be such that there is no choking point / bottleneck anywhere in the system (end-to-end) which can affect the performance / SLAs.

Subject to the fulfilment of the obligations of the Service Provider as provided for in sub clause (a) and (b) above, in the event that such warranties cannot be enforced by VSCDL, the Service Provider will enforce such warranties on behalf of VSCDL and pass on to VSCDL, the benefit of any other remedy received in relation to such warranties.

- c. Notwithstanding what has been stated elsewhere in this Agreement and the Schedules attached herein, in the event the Systems Integrator is unable to meet the obligations pursuant to the implementation of the Project, Operations and Maintenance Services and any related scope of work as stated in this Agreement and the Schedules attached herein, and has failed to cure such default within thirty days from the occurrence of such default, VSCDL will have the option to invoke the Performance Guarantee after serving a written notice of thirty (30) days on the Systems Integrator.

14. Force Majeure and Vandalism

In the event that any damages to items due to vandalism (physical Majeure attack by public, tampering of equipment by VSCDL staff and damage due to accidents) or due to Force Majeure events (such as earthquake, fire, natural calamities, war, act of God) of any kind during warranty period and maintenance period shall be the liability of VSCDL. In such case, VSCDL shall request the Systems Integrator (SI) to repair/replace the damaged unit and reinstall the same. All costs towards the same shall be reimbursed by VSCDL to the Systems Integrator less of insurance proceeds if need of replacement so arise then replacement shall be on tender rates only.

The Systems Integrator shall not be liable for forfeiture of its Performance Guarantee, imposition of liquidated damages or termination for default, if and to the extent that it's delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure. For purposes of this Clause, "Force Majeure" means an event beyond the "reasonable" control of the Service Provider, not involving the Systems Integrator's fault or negligence and not foreseeable. Such events may include Acts of God and Acts of Government of India in their sovereign capacity.

For the SI to take benefit of this clause it is a condition precedent that the SI must promptly notify the VSCDL in writing of such conditions and the cause thereof within 7 calendar days of the Force Majeure event arising. VSCDL, or the consultant / committee appointed by the VSCDL shall study the submission of the SI and inform whether the situation can be qualified one of Force Majeure. Unless otherwise directed by the VSCDL in writing, the SI shall continue to perform its obligations under the resultant Agreement as far as it is reasonably practical, and shall seek all reasonable alternative means for performance of services not prevented by the existence of a Force Majeure event.

For the VSCDL to take benefit of this clause, VSCDL may specify SI in writing of such conditions within 7 days of the force majeure event arising. Under such conditions VSCDL will delay any payment mentioned in this agreement and such payments would be processed later after closure of such events.

In the event of delay in performance attributable to the presence of a force majeure event, the time for performance shall be extended by a period(s) equivalent to the duration of such delay. If the duration of delay continues beyond a period of 30 days, VSCDL and the SI shall hold consultations with each other in an endeavour to find a solution to the problem.

Notwithstanding anything to the contrary mentioned above, the SI agrees that the decision of the VSCDL shall be final and binding. .

15. Resolution of Disputes

VSCDL and the SI shall make every effort to resolve amicably, by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the Agreement. If after 30 days from the commencement of such informal negotiations, VSCDL and the SI are unable to resolve amicably such dispute, the matter shall be referred to a Tribunal of three (3) Arbitrators, constituted as per the terms of and under the (Indian) Arbitration and Conciliation Act, 1996. Each party to the contract shall appoint/ nominate one Arbitrator each, the two Arbitrators so appointed/ nominated by the VSCDL and the SI herein shall together choose the third Arbitrator, who shall be the Presiding Arbitrator of the Tribunal. The consortium of the three Arbitrators shall form the Arbitral Tribunal. Proceedings under this clause shall be subject to applicable law of the Arbitration and Reconciliation Act, 1996 and the seat and venue of such arbitration shall be Vadodara. The proceedings shall be undertaken in English. The arbitration award shall be final and binding on the Parties. Cost of arbitration shall be borne by each party proportionately. However, expenses incurred by each party in connection with the preparation, presentation shall be borne by the party itself. The provisions of this clause shall survive termination of this Agreement. Parties agree that pending the submission of and / or decision on a dispute and until the Arbitral Award is published, the Parties shall continue to perform their respective obligations under this Agreement, without prejudice to its rights, interest and entitlements, till the final decision / Award.

16. Limitation of Liability towards VSCDL

The SI's liability under the resultant Agreement shall be determined as per the law in force for the time being. The SI shall be liable to the VSCDL for loss or damage occurred or caused or likely to occur on account of any act of omission on the part of the SI and its employees, including loss caused to VSCDL on account of defect in goods or deficiency in services on the part of SI or his agents or any person/persons claiming through or under said SI. However, SI's cumulative liability for all its obligations under the contract shall not exceed the value of the charges payable by VSCDL within the remaining duration of the contract term from the day claim is raised.

This limitation of liability shall not limit the SI's liability, if any, for damage to Third Parties caused by the SI or any person or firm acting on behalf of the SI in carrying out the scope of work envisaged herein.

17. Conflict of Interest

A conflict of interest is any situation that might cause an impartial observer to reasonably question whether SI actions are influenced by considerations of SI firm's personal interest and benefit at the cost of Government and/or VSCDL.

The SI shall disclose to the VSCDL in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for the Systems Integrator or its Team) in the course of performing Services as soon as it becomes aware of such a conflict. However, SI shall hold VSCDL's interest paramount, without any consideration for future work, and strictly avoid conflict of interest with other assignments.

18. Data Ownership

All the data created as the part of the project shall be owned by VSCDL. The SI shall take utmost care in maintaining security, confidentiality and backup of this data. Access to the data / systems shall be given by the SI only as per the IT Security Policy, approved by VSCDL. VSCDL / its authorized representative(s) shall conduct periodic / surprise security reviews and audits, to ensure the compliance by the SI vendor to data / system security.

19. Intellectual Property Rights

- (A) For the customized solution developed for the project, IPR of the solution would belong exclusively to the VSCDL. The SI shall transfer the source code to VSCDL at the stage of successful implementation of the respective smart element. SI shall also submit all the necessary instructions for incorporating any modification / changes in the software and its compilation into executable / installable product. VSCDL

may permit the SI, right to use the customized software for any similar project being executed by the same SI, with payment of reasonable royalty to VSCDL for the same. The SI hereby understands and agrees that such permission to use a customized software may be given at the discretion of VSCDL and is not a right of the SI.

- (B) Deliverables provided to VSCDL by Service Provider during the course of its performance under this Agreement, all rights, title and interest in and to such Deliverables, shall, as between Service Provider and VSCDL, immediately upon creation, vest in VSCDL. To the extent that the Service Provider Proprietary Information is incorporated within the Deliverables, Service Provider and its employees engaged hereby grant to VSCDL a worldwide, perpetual, irrevocable, non-exclusive, royalty-free, fully transferable, paid-up right and license to use, copy, modify (or have modified), use and copy derivative works for the benefit of and internal use of VSCDL.
- (C) The SI shall be obliged to ensure that all approvals, registrations, filings, licenses, permits, and rights, including all IP rights, which are, inter-alia, necessary for use and protection of the deliverables, goods, services, applications, services, etc. provided by the SI / subcontractors under this Agreement shall be acquired in the name of the VSCDL and SI shall use such licenses till the subsistence of this Agreement on behalf of VSCDL solely for the purpose of execution of any of its obligations under the terms of this Agreement. However, subsequent to the term of this Agreement, such approvals, etc. shall endure to the exclusive benefit of the VSCDL.
- (D) SI shall not copy, reproduce, translate, adapt, vary, modify, disassemble, decompile or reverse engineer or otherwise deal with or cause to reduce the value of the Assets except as expressly authorized by VSCDL in writing.

20. Fraud and Corruption

VSCDL requires that SI must observe the highest standards of ethics during the execution of the contract. In pursuance of this policy, VSCDL defines, for the purpose of this provision, the terms set forth as follows:

- a. "Corrupt practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of VSCDL in contract executions.
- b. "Fraudulent practice" means a misrepresentation of facts, in order to influence a procurement process or the execution of a contract, to VSCDL, and includes collusive practice among bidders (prior to or after Proposal submission) designed to establish Proposal prices at artificially high or non-competitive levels and to deprive VSCDL of the benefits of free and open competition.
- c. "Unfair trade practices" means supply of services different from what is ordered on, or change in the Scope of Work which is given by the VSCDL in Volume II.
- d. "Coercive Practices" means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in the execution of contract.

If it is noticed that the SI has indulged into the Corrupt / Fraudulent / Unfair / Coercive practices or any similar prejudicial practices, it will be a sufficient ground for VSCDL for termination of the contract and initiate black-listing of the vendor.

21. Exit Management

(i) Exit Management Purpose

This clause sets out the provisions, which will apply during Exit Management period. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Clause.

The exit management period starts, in case of expiry of contract, at least 6 months prior to the date when the contract comes to an end or in case of termination of contract, on the date when the notice of termination is sent to the SI. The exit management period ends on the date agreed upon by VSCDL or six months after the beginning of the exit management period, whichever is earlier.

(ii) Confidential Information, Security and Data

Systems Integrator will promptly on the commencement of the exit management period, supply to the VSCDL or its nominated agencies the following:

- a) Information relating to the current services rendered and performance data relating to the performance of the services; documentation relating to CYBER SECURITY Project, Project's Intellectual Property Rights; any other data and confidential information related to the Project;
- b) Project data as is reasonably required for purposes of the project or for transitioning of the services to its Replacing Successful Bidder in a readily available format.
- c) All other information, including but not limited to documents, records and agreements, relating to the services reasonably necessary to enable the VSCDL and its nominated agencies, or its Replacing Vendor to carry out due diligence in order to transition the provision of the Services to VSCDL or its nominated agencies, or its Replacing Vendor (as the case may be).
- d) The SI shall provide a one (1) week training at the office of the SI to the Replacement Service Provider and it shall be obligation of VSCDL to ensure that the necessary officials of the Replacement Service Provider attend the training. Any training provided beyond the aforementioned period one (1) week shall be chargeable at the instance of the SI.
- e)

(iii) Employees

Promptly on reasonable request at any time during the exit management period, the SI shall, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide to VSCDL a list of all employees (with job titles and communication address) of the SI, dedicated to providing the services at the commencement of the exit management period;

To the extent that any Transfer Regulation does not apply to any employee of the SI VSCDL or Replacing Vendor may make an offer of contract for services to such employee of the SI and the SI shall not enforce or impose any contractual provision that would prevent any such employee from being hired by the VSCDL or any Replacing Vendor.

(iv) Rights of Access to Information

At any time during the exit management period, the SI will be obliged to provide an access of information to VSCDL and / or any Replacing Vendor in order to make an inventory of the Assets (including hardware / Software / Active / passive), documentations, manuals, catalogues, archive data, Live data, policy documents or any other material related to the ALEPS Project.

(v) Exit Management Plan

The SI shall provide VSCDL with a recommended exit management plan ("Exit Management Plan") within 90 days of signing of the contract, which shall deal with at least the following aspects of exit management in relation to the SLA as a whole and in relation to the project implementation, the operation and management SLA and scope of work definition.

- a) A detailed program of the transfer process that could be used in conjunction with a Replacement Vendor including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;
- b) Plans for the communication with SI, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on Project's operations as a result of undertaking the transfer;
- c) Plans for provision of contingent support to the CYBER SECURITY project and Replacement Vendor for a reasonable period (minimum one month) after transfer.
- d) SI shall re-draft the Exit Management Plan annually to ensure that it is kept relevant and up to date.

- e) Each Exit Management Plan shall be presented by the SI to and approved by VSCDL or its nominated agencies.
- f) The terms of payment as stated in the Terms of Payment Schedule include the costs of the SI complying with its obligations under this Schedule.
- g) During the exit management period, the SI shall use its best efforts to deliver the services.
- h) Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.

(vi) Transfer Cost

On premature termination of the contract for reasons other than those mentioned in Section _____ (Termination for Default), the SI shall be paid the depreciated book value of the infrastructure cost and the other assets (as per the Asset Register). The depreciation rates and method followed will be as per Income Tax Rules.

Note: Amount to be payable to SI on premature termination of contract =

Pending amount to be paid against services delivered + Depreciated Book Value of the Assets as per Income Tax Rules – Applicable Penalty / Liquidated Damages

22. Termination of Contract

VSCDL may, without prejudice to any other remedy under this Contract and applicable law, reserves the right to terminate for breach of contract by providing a written notice of 30 days stating the reason for default to the SI and as it deems fit, terminate the contract either in whole or in part:

- If the SI fails to deliver any or all of the project requirements / operationalization / go-live of the project within the time frame specified in the contract; or
- If the SI fails to perform any other obligation(s) under the contract.

Prior to providing a notice of termination to the SI, VSCDL shall provide the SI with a written notice of 30 days instructing the SI to cure any breach/ default of the Contract, if VSCDL is of the view that the breach may be rectified.

On failure of the SI to rectify such breach within time frame specified, VSCDL may terminate the contract with immediate effect by providing a written notice (Show cause notice / any other notice) to the SI. Such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to VSCDL. In such event the SI shall be liable for penalty/liquidated damages imposed by the VSCDL. The performance Guarantee shall be forfeited by the VSCDL.

Termination for Insolvency

VSCDL may at any time terminate the contract by giving written notice to the SI on following conditions, without compensation to the SI, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to VSCDL:

- 1) if the SI becomes bankrupt, otherwise insolvent, or apply for insolvency, voluntarily or otherwise;
- 2) If the SI undergoing any NCLT proceedings In the event of termination as per mentioned clause VSCDL reserves the right to take suitable action against SI against their default including revoking the PBG and imposing other damages. Note: Consortium is not allowed for this project

In the event of termination as per mentioned clause VSCDL reserves the right to take suitable action against SI against their default including revoking the PBG and imposing other damages.

Consequences of Termination

In the event of termination of this contract, VSCDL is entitled to impose any such obligations of the SI in relation to the requirement of the contract and issue any clarifications as may be necessary to ensure an efficient transition and effective continuity of the services which the SI shall be obliged to comply with and take all available steps to minimize the loss resulting from that termination/ breach, and further allow and provide all such assistance to VSCDL and/ or succeeding vendor, as may be required, to take over the obligations of the SI in relation to the

execution / continued execution of the requirements of this contract.

Plans and drawings

All plans, drawings, specifications, designs, reports and other documents prepared by the Vendor in the execution of the contract shall become and remain the property of VSCDL and before termination or expiration of this contract the SI shall deliver all such documents, prepared under this contract along with a detailed inventory thereof, to VSCDL.

23. Tech Refresh

. In case, additional costs and expenses are incurred in refreshing the technology, SI shall duly inform VSCDL, which may at its discretion agree to bear some of the additional costs. The SI shall only refresh the technology provided under the Contract and shall not be responsible to refresh technology in any way if the technology provided by the SI is altered, changed, modified, clubbed, mixed with other services or product, by any third party or agent.

24. Miscellaneous

a) Confidentiality

"Confidential Information" means all information including project data (whether in written, oral, electronic or other format) which relates to the technical, financial and operational affairs, business rules, citizen information, video footages, alert information, any police department data, products, processes, data, crime / criminal secrets, design rights, know-how and personnel of each Party and its affiliates which is disclosed to or otherwise learned by the other Party subcontractors (whether a Party to the contract or to the SLA) in the course of or in connection with the contract (including without limitation such information received during negotiations, location visits and meetings in connection with the contract or to the SLA) or pursuant to the contract to be signed subsequently.

Except with the prior written permission of VSCDL, the Systems Integrator (and its Personnel shall not disclose such confidential information to any person or entity not expected to know such information by default of being associated with the project, nor shall the Systems Integrator and its personnel make public the recommendations formulated in the course of, or as a result of the Project.

- a. The SI recognizes that during the term of this Agreement, sensitive data will be procured and made available to it, its sub-contractors & agents, and others working for or under the SI. Disclosure or usage of the data by any such recipient may constitute a breach of law applicable causing harm not only to VMC/VSCDL whose data is used but also to its stakeholders. The SI, its sub-contractors & agents are required to demonstrate utmost care, sensitivity and strict confidentiality. Any breach of this Article will result in VSCDL and its nominees receiving a right to seek injunctive relief and damages from the SI and SI shall fully indemnify VSCDL if any third person or entity initiates any proceedings for breach of privacy or misuse of data.
- b. Each Party agrees as to any Confidential Information disclosed by a Party to this Agreement (the "Discloser") to the other Party to this Agreement (the "Recipient") and
 - i. to take such steps necessary to protect the Discloser's Confidential information from unauthorized use, reproduction & disclosure, as the Recipient takes in relation to its own Confidential Information of the same type, but in no event less than reasonable care;
 - ii. to use such Confidential Information only for the purposes of this Agreement or as otherwise expressly permitted or expressly required by this Agreement or as otherwise permitted by the Discloser in writing;
 - iii. not, without the Discloser's prior written consent, to copy the Confidential Information cause or allow it to be copied, directly or indirectly, in whole or in part, except as otherwise expressly provided in this Agreement, or as required in connection with Recipient's use as permitted under this Article, or as needed for the purposes of this Agreement, or as needed for the purposes

- of this Agreement, provided that any proprietary legends & notices (whether of the Discloser or of a Third Party) are not removed or obscured;
- iv. Not, to disclose, transfer, publish or communicate the Confidential Information in any manner, without the Discloser's prior written consent, to any person except as permitted under this Agreement.
- c. The restrictions of this Article shall not apply to confidential Information that:
- i. is or becomes generally available to the public through no breach of this Article by the Recipient;
 - ii. was in the recipient's possession free of any obligation of confidence prior to the time of receipt of it by the Recipient hereunder;
 - iii. is developed by the recipient independently of any of discloser's confidential information;
 - iv. Is rightfully obtained by the recipient from third parties authorized at that time to make such disclosure without restriction;
 - v. is identified in writing by the discloser as no longer proprietary or confidential; or is required to be disclosed by law, regulation or Court Order, provided that the recipient gives prompt written notice to the Discloser of such legal & regulatory requirement to disclose so as to allow the Discloser reasonable opportunity to contest such disclosure.
- d. To the extent that such disclosure is required for the purposes of this Agreement, either Party may disclose Confidential Information to:
- i. its employees, agents & independent contractors & to any of its affiliates and their respective independent contractors or employees;
 - ii. its professional advisors & auditors, who require access for the purposes of this Agreement, whom the relevant Party has informed of its obligations under this Article and in respect of whom the relevant Party has informed of its obligations under this Article has used commercially reasonable efforts to ensure that they are contractually obliged to keep such Confidential Information confidential on terms substantially the same as set forth in this Article. Either Party may also disclose confidential Information or any entity with the other Party's prior written consent.
- e. The provisions of this Article shall survive three years post expiration or any earlier termination of this Agreement.
- f. Confidential Information shall be & remain the property of the discloser and nothing in this Article shall be construed to grant either Party any right or license with respect to the other Party's confidential Information otherwise than as is expressly set out in this Agreement.
- g. Subject as otherwise expressly provide in this Agreement all Confidential Information in tangible or electronic form under the control of the Recipient shall either be destroyed, erased or returned to the Discloser promptly upon the earlier of: (i) the written request of the Disclose, or, (ii) termination or expiry of this Agreement or, in respect of the SLAs, the termination or expiry of the SLAs. Notwithstanding the forgoing, both Parties may retain, subject to the terms of this Article, reasonable number of copies of the other Party's Confidential Information solely for confirmation of compliance with the confidentiality obligations of this Agreement.
- h. Neither Party is restricted by the provisions of this clause from using (including using to provide products or perform services on behalf of third Parties) any ideas, concepts, know-how and techniques that are related to the Recipient's employees or agents (and not intentionally memorized for the purpose of later recording or use) (collectively, the "residuals"). This Article shall not permit the disclosure or use by either Party or any financial (including business plans), statistical, product, personnel or customer data or the other Party. Each party agrees not to disclose the source of the Residuals.
- i. Both Parties agree that monetary damages would not be a sufficient remedy for any breach of this clause by the other Party and that VSCDL & Service Provider, as appropriate, shall be entitled to equitable relief, including injunction & specific performance as a remedy for any such breach. Such remedies shall not be deemed to be the exclusive remedies for a breach by a Party of this clause, but shall be in addition to all other remedies available at law or equity to the damaged Party.
- j. in connection with the Services, Service Provider may from time to time undertake one or more quality assessment reviews for the purpose of improving the VSCDL Project. In order for such

reviews to be frank and candid, for the greatest benefit to both VSCDL & SI, they shall be kept confidential to the greatest extent possible. The Parties agree that any documentation created in connection with such quality assessment reviews shall be Confidential Information of SI and VSCDL which is licensed to VSCDL for any internal use and such documentation or the results of such reviews be discoverable or admissible (or used for any purpose) in any arbitration or legal proceedings against SI related to this Agreement or the Services.

A Non-disclosure agreement shall be signed separately between the Systems Integrator and VSCDL.

b) Standards of Performance

The SI shall provide the services and carry out their obligations under the Contract with due diligence, efficiency and professionalism/ethics in accordance with generally accepted professional standards and practices. The SI shall always act in respect of any matter relating to this contract. The SI shall abide by all the provisions/Acts/Rules/Regulations, Standing Orders, etc. of Information Technology as prevalent in the country. The SI shall also conform to the standards laid down by VMC/VSCDL/Government of Gujarat/Government of India from time to time.

c) Sub Contracts

All the personnel working on the project and having access to the Servers / data should be on payroll of the Systems Integrator. Sub-contracting/outsourcing would be allowed only for work like

- Passive Networking and Civil Work during implementation
- FMS staff for non- IT support during post-implementation
- Services of professional architect for design of command / viewing centres
- Services delivered by the respective Product Vendors / OEMs

The SI is expected to provide details of the sub-contractors for the work which is allowed as mentioned in the clause. Use of personnel not on payroll of the SI shall be considered as sub-contracting.

The SI shall take prior approval from VSCDL for sub-contracting any allowed work as mentioned in clause, if not already specified in the proposal and approved by VSCDL. Such sub-contracting shall not relieve the SI from any liability or obligation under the Contract. The SI shall solely responsible for the work carried out by subcontracting under the contract.

d) Care to be taken while working at Public Place

SI should follow instructions issued by *concerned Competent Authority and* VSCDL from time to time for carrying out work at public places. SI should ensure that there is no damage caused to any private or public property. In case such damage is caused, SI shall immediately bring it to the notice of concerned organization and VSCDL in writing and pay necessary charges towards fixing of the damage. SI should also ensure that no traffic *congestion*/public inconvenience is caused while carrying out work at public places.

SI shall ensure that its employees/representatives don't breach privacy of any citizen or establishment during the course of execution or maintenance of the project.

e) Compliance with Labour regulations

For all employees, workmen, working with SI, either of payroll or as sub-contractors, the SI shall pay fair and reasonable and shall comply with the provisions set forth under law, including the Minimum Wages Act and the Contract Labour Act 1970. The VSCDL shall in no way be held liable for any breach, violation or non-compliance by the SI of any of the laws, regulations, and policies governing labour, employment, insurance, workmen compensation, industrial disputes, etc.

f) Independent Contractor

Nothing in this Agreement shall be construed as establishing or implying any partnership or joint venture or *employment relationship* between the Parties to this Agreement. Except as expressly stated in this Agreement nothing in this Agreement shall be deemed to constitute any Party as the agent of any other Party or authorizes either Party (i) to incur any expenses on behalf of the other Party, (ii) to enter into any engagement or make any representation or warranty on behalf of the other Party, (iii) to pledge the credit of or otherwise bind or oblige the other Party, or (iv) to commit the other Party in any manner whatsoever in each case without obtaining the other Party's prior written consent.

g) Waiver

A waiver of any provision or breach of this Agreement must be in writing and signed by an authorized official of the Party executing the same. No such waiver shall be construed to affect or imply a subsequent waiver of the same provision or subsequent breach of this Agreement.

h) Notices

Any notice or other document, which may be given by either Party under this Agreement, shall be given in writing in person or by pre-paid recorded delivery post.

In relation to a notice given under this Agreement, any such notice or other document shall be addressed to the other Party's principal or registered office address as set out below

VSCDL:

CEO, VSCDL

Systems Integrator:

Tel: _____
Fax: _____

Any notice or other document shall be deemed to have been given to the other Party when delivered (if delivered in person) between the hours of 9.30 am and 5.30 pm at the address of the other Party set forth above or on the next working day thereafter if delivered outside such hours, and 7 calendar days from the date of posting (if by letter).

i) Performance Guarantee

The SI shall submit two unconditional and irrevocable Performances Bank Guarantee(s) (PBGs) from a list of approved banks; one PBG for the implementation phase valid for 1 years, and one PBG for operations phase for 5 years from go-live. The implementation phase PBG will be 10% of Capex and operations phase PBG will be 10% of Opex. The performance guarantee shall be renewed & maintained by the SI for the term of the agreement & extension, if any. The performance guarantee shall be forfeited / liquidated by the VSCDL as a penalty in the event of failure to complete obligations or breach of any of the conditions by the SI.

j) Personnel/Employees

- i. Personnel/employees assigned by the SI to perform the services shall be employees of SI or its sub-contractors, and under no circumstances will such personnel be considered as employees of VSCDL. SI shall have the sole responsibility for supervision & control of its personnel & for payment of such personnel's employee's entire compensation, including salary, legal deductions withholding of income taxes & social security taxes, worker's compensation, employee & disability benefits & the like & shall be responsible for all employer obligations under all laws as applicable from time to time. The VSCDL shall not be responsible for the above issues concerning to personnel of SI.
- ii. SI shall use its best efforts to ensure that sufficient SI personnel are employed to perform the Services, and that, such personnel have appropriate qualifications to perform the Services. VSCDL or its nominated agencies shall have the right to require the removal or replacement of any SI

personnel performing work under this Agreement. In the event that VSCDL requests that any SI personnel be replaced, the substitution of such personnel shall be accomplished pursuant to a mutually agreed upon schedule & upon clearance of the personnel based on profile review & upon schedule & upon clearance of the personnel based on profile review & personal interview by VSCDL or its nominated agencies, within not later than 30 working days. Service Provider shall depute quality team for the project & as per requirements, VSCDL shall have the right to ask Service Provider to change the team.

- iii. Management (Regional Head / VP level officer) of SI need to be involved in the project monitoring and should attend the review meeting at least once in a month.
- iv. The profiles of resources proposed by SI in the technical proposal, which are considered for Technical bid evaluation, shall be construed as 'Key Personnel' and the SI shall not remove such personnel without the prior written consent of VSCDL. For any changes to the proposed resources, SI shall provide equivalent or better resources (in terms of qualification & experience) in consultation with VSCDL.
- v. Except as stated in this clause, nothing in this Agreement will limit the ability of SI freely to assign or reassign its employees; provided that SI shall be responsible, at its expense, for transferring all appropriate knowledge from personnel being replaced to their replacements. VSCDL shall have the right to review and approve Service Provider's plan for any such knowledge transfer. SI shall maintain the same standards for skills & professionalism among replacement personnel as in personnel being replaced.
- vi. Each Party shall be responsible for the performance of all its obligations under this Agreement and shall be liable for the acts & omissions of its employees & agents in connection therewith.

k) Variations and Further Assurance

- a. No amendment, variation or other change to this Agreement or the SLAs shall be valid unless made in writing and signed by the duly authorized representatives of the Parties to this Agreement.
- b. Each Party to this Agreement or the SLAs agree to enter into or execute, without limitation, whatever other agreement, document, consent & waiver & to do all other things which shall or may be reasonably required to complete & deliver the obligations set out in the Agreement or the SLAs.

l) Severability and Waiver

- a. if any provision of this Agreement or the SLAs, or any part thereof, shall be found by any court or administrative body of competent jurisdiction to be illegal, invalid or unenforceable the illegality, invalidity or unenforceability of such provision or part provision shall not affect the other provisions of this Agreement or the SLAs or the remainder of the provisions in question which shall remain in full force and effect. The relevant Parties shall negotiate in good faith in order to agree to substitute any illegal, invalid or unenforceable provision with a valid & enforceable provision which achieves to the greatest extent possible the economic, legal & commercial objectives of the illegal, invalid or unenforceable provision or part provision within 7 working days of the reporting of this dispute.
- b. No failure to exercise or enforce and no delay in exercising or enforcing on the part of either Party to this Agreement or the SLAs of any right, remedy or provision of this Agreement or the SLAs shall operate as a waiver of such right, remedy or provision in any future application nor shall any single or partial exercise or enforcement of any right, remedy or provision preclude any other or further exercise or enforcement of any other right, remedy or provision.

m) Entire Agreement

This MSA, the SLAs and all schedules appended thereto & the contents & specifications of the Volumes I & II, of the RFP subsequent corrigenda issued thereon & clarification (undertakings) accepted by the VSCDL constitute the entire agreement between the Parties with respect to their subject matter.

n) Survivability

The termination or expiry of this Agreement or the SLAs for any reason shall not affect or prejudice any terms of this Agreement, or the rights of the Parties under them which are either expressly or by implication intended to come into effect or continue in effect after such expiry or termination.

- o) The stamp duty payable for the contract shall be borne by the Systems Integrator.
- p) Deliverables will be deemed to be accepted by VSCDL if no communication from the department is made to the SI after 30 days of delivery, provided the delivery is made to the designated officer and clearly highlighted in at least 3 weekly project progress reports

25. Applicable Law

The contract shall be governed by the laws and procedures prescribed by the Laws prevailing and in force in India, within the framework of applicable legislation and enactment made from time to time concerning such commercial dealings/processing. All legal disputes are subject to the jurisdiction of Vadodara courts only.

IN WITNESS whereof the parties hereto have signed this on the day, month and year first herein above written.

Signed, sealed and delivered

By _____,

For and on behalf of the **Governor of the
State of Gujarat**

Signed, sealed and delivered

By _____,

For and on behalf of the “Systems Integrator”,

Witnesses:

(1)

(2)

Attachments to the Agreement:

- 1) Scope of Services for the Systems Integrator (Annexure I)
- 2) Detail Commercial proposal of the Systems Integrator accepted by VSCDL (Annexure II)
- 3) SLA to be adhered by the Systems Integrator (Annexure III)
- 4) Corrigendum Document published by VSCDL subsequent to the RFP for this work (Annexure IV)
- 5) RFP Document of VSCDL for this work (Annexure V)
- 6) LoI issued by the VSCDL to the successful bidder (Annexure VI)

The successful bidder’s “Technical Proposal” and “Commercial Proposal” submitted in response to the RFP (Annexure VII)

17 Annexure IX: Non-Disclosure Agreement

<<To be printed on Stamp Paper of Rs 300>>

To be Signed by both the parties during contract signing

NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement ('Agreement') is made at Vadodara and is effective from ____
"effective date".

Between

Vadodara Smart City Development Limited, a Company incorporated under the
..... **and** having its registered office at Vadodara Municipal Corporation, Khanderao
Market, Vadodara – 390 001, Gujarat, hereinafter referred to as 'VSCDL' or the "First Party" which
expression shall, unless it be repugnant to the context or meaning thereof be deemed to mean and
include their successors and executors) of the **First Part**;

And

Selected Bidder, a company incorporated under the Companies Act, 1956, having Corporate Identity
Number or CIN: _____ and its registered office
at _____, hereinafter
referred to as "SI" or the "SECOND PARTY". which expression shall, unless it be repugnant to the
context or meaning thereof be deemed to mean and include their successors and executors) of the
Second Part;

WHEREAS A.

VSCDL and SI, shall be hereinafter individually referred to as "party" and/or as defined hereinabove
and collectively as the "parties". Note: Consortium is not allowed for this project

1. Background

VSCDL has set up an Integrated Command Control Center (ICCC) in Vadodara in connection with
the Smart City Mission of MoUHA, which is partly funded by Smart City Mission (Government of
India), Government of Gujarat and Vadodara Municipal Corporation. The SECOND PARTY i.e. SI
has been selected as System Integrator for this project through public procurement (tendering)
process via RFP no. _____ issued on _____, for Cyber Security

Solution for 5 years as per contract signed between the two parties hereto. For this purpose, the Parties hereto may have access to all information/data generated under this project, including Integrated Command and Control Centre running at Vadodara Smart city and the Parties shall be required to disclose certain confidential information to each other. As per Clause 22 (a) – Confidentiality of the contract agreement between VSCDL and SI, a Non- Disclosure Agreement needs to be signed between FIRST PARTY and SECOND PARTY.

VSCDL and SI agree that the following terms and conditions shall apply when VSCDL i.e. First Party / Disclosing Party discloses confidential information to the SI i.e. Second Party/Receiving Party under this Agreement. The objective of this Agreement is to provide appropriate protection for such information whilst maintaining the parties' ability to conduct their respective businesses.

2. Definitions

In this Agreement, the following terms shall have the following meanings:

‘Confidential Information’ means information as disclosed by Disclosing Party to the Receiving Party which included all information including Project Data (whether in written, oral, electronic or other format) which relates to the technical, financial and operational affairs, business rules, citizen information, video footages, alert information, any police department data, products, processes, data, crime / criminal secrets, design rights, knowhow and personnel of each Party and its affiliates which is disclosed to or otherwise learned by the Receiving Party or subcontractors (whether a Party to the contract or to the SLA) in the course of or in connection with the contract (including without limitation such information received during negotiations, location visits and meetings in connection with the contract or to the SLA) or pursuant to the contract to be signed subsequently. which is not generally known to the public, in written, oral, or in any other form (including such tangible forms as written or printed documents and computer disks or tapes, whether machine or user readable), that First Party designates as being confidential (express and/or implied) or that, under the circumstances surrounding disclosure, should reasonably be considered as confidential and any other information disclosed or submitted whether prior to the date of this Agreement or thereafter including without limitation, the information on the contents and existence of this Agreement and analysis, compilations, studies and other documents prepared by First Party or its representative in relation to or arising out of the Smart City Project or which contain or otherwise reflect or are generated from any Confidential Information or otherwise acquired/ accessed by the second party during the course of dealings between the Parties or otherwise in connection with the Purpose.. Confidential Information disclosed to a Receiving Party by the Disclosing Party's subsidiary, advisor, agent or representative is covered by this Agreement. Confidential Information means any information disclosed by or on behalf of VSCDL to the SECOND PARTY, which (i) if disclosed in tangible form is marked confidential or (ii) if disclosed otherwise than in tangible form is confirmed in writing as being confidential or (iii) if disclosed in tangible form or otherwise, is manifestly confidential.

‘VSCDL’ means the “Disclosing Party” and/or “Discloser” for the purposes of this Agreement disclosing the Confidential Information.

‘SECOND PARTY Firms’ means any entity (whether or not incorporated) which carries on business under a name which includes all or part of the SECOND PARTY name or is otherwise within (or associated or connected with an entity within) or is a correspondent firm of the world-wide network of the SECOND PARTY firms.

‘Receiving Party’ and/or “Recipient” means the Second Party to this Agreement to whom the Confidential Information is disclosed.

3. Supply and Use of Information:

- a. In consideration of the disclosures contemplated by, and of the respective obligations set out in this Agreement, the Receiving Party agrees, save as otherwise expressly permitted by this Agreement:
 - i. To keep the Confidential Information, confidential;
 - ii. Use the confidential information in connection with the Purpose, pursuant to which a given item of Confidential Information was disclosed;
 - iii. Not to use the Confidential Information except in connection with the Purpose; and
 - iv. Not to disclose the Confidential Information to any third party except for a party in the consortium of firms intending to submit the working on the project.
- b. The Confidential Information divulged by the Disclosing Party to the Receiving Party will be received and treated by the Receiving Party as strictly confidential and the Receiving Party shall not, without the prior written consent of the Disclosing Party or as expressly permitted herein, disclose or make available to any other person, or use or allow others to disclose or use, the Confidential Information in any manner, whatsoever, other than for the sole purpose provided hereunder
- c. The Receiving Party shall use Confidential Information only for the purpose for which it was disclosed and shall not use or exploit such information for their own benefit or the benefit of a third party without prior written consent of Disclosing Party.
- d. In the case of Confidential Information that is disclosed only orally, the Disclosing Party shall, within seven days after such disclosure, deliver to the Receiving Party a brief written description of such Confidential Information; identifying the place and date of such oral disclosure and the names of the representatives of the Receiving Party to whom such disclosure was made. It is expected that such information will bear a legend or label of “Confidential” or other similar designation manifesting intent that the information is confidential.
- e. Each party confirms that it and its Affiliates (or, in case of SECOND PARTY, other SECOND PARTY Firms) have the right to disclose any Confidential Information that they provide to the other under this Agreement. Receiving Party may disclose such confidential information to its employees, affiliates and consultants with a need-to-know that are bound by substantially similar requirements which are at least as restrictive as this Agreement.
- f. The Receiving Party undertakes to impose the confidentiality obligations on all its directors, officers, and employees or other persons who work for the Recipient or under its direction and control
- g. Upon the Disclosing Party’s request, the Receiving Party will promptly return to the Disclosing Party’s all tangible items containing or consisting of the Disclosing Party’s Confidential Information and all copies thereof.

The obligation contained above shall survive any termination/expiration of the Agreement.

4. Confidentiality

“Confidential Information” means the Confidential Information as defined in Clause 2 definitions hereinabove.

Except with the prior written permission of Disclosing Party, the Receiving Party) and its Personnel shall not disclose such confidential information to any person or entity not expected to know such information by default of being associated with the project, nor shall the Receiving Party (and it's Personnel make public the recommendations formulated in the course of, or as a result of the Project.

h. SI recognizes that during the term of this Agreement, sensitive data will be procured and made available to it, its sub-contractors & agents, and others working for or under SI. Disclosure or usage of the data by any such recipient may constitute a breach of law applicable causing harm not only to VSCDL/ VMC whose data is used but also to its stakeholders. SI, its sub-contractors & agents are required to demonstrate utmost care, sensitivity and strict confidentiality. Any breach of this Article will result in VSCDL and its nominees receiving a right to seek injunctive relief and damages from SI.

i. This Agreement shall not apply to Confidential Information which:

- i. Is or becomes generally available to the public through no breach of this Agreement by the Recipient;
- ii. was in the recipient's possession free of any obligation of confidence prior to the time of receipt of it by the Recipient hereunder;
- iii. is developed by the recipient independently of any of discloser's confidential information;
- iv. Is rightfully obtained by the recipient from third parties authorized at that time to make such disclosure without restriction of confidentiality obligations;

is identified in writing by the discloser as no longer proprietary or confidential; or is required to be disclosed by law, regulation or Court Order, provided that the recipient gives prompt written notice to the Discloser of such legal & regulatory requirement to disclose so as to allow the Discloser reasonable opportunity to seek a protective order with respect to the Confidential Information required to be disclosed. The Receiving Party will promptly cooperate with and assist First Party in connection with obtaining such protective order.

j. To the extent that such disclosure is required for the purposes of this Agreement, either Party may disclose Confidential Information to:

- i. its employees, agents & independent contractors & to any of its affiliates and their respective independent contractors or employees;
- ii. its professional advisors & auditors, who require access for the purposes of this Agreement, whom the relevant Party has informed of its obligations under this Article and in respect of whom the relevant Party has informed of its obligations under this Article has used commercially reasonable efforts to ensure that they are contractually

obliged to keep such Confidential Information confidential on terms substantially the same as set forth in this Article. Either Party may also disclose confidential Information to any entity with the other Party's prior written consent.

- k. The provisions of this Agreement shall survive expiration or any earlier termination of this Agreement and shall be for perpetuity.
- l. Confidential Information shall be & remain the property of the discloser and nothing in this Agreement shall be construed to grant either Party any right or license with respect to the other Party's confidential Information otherwise than as is expressly set out in this Agreement.
- m. Subject as otherwise expressly provide in this Agreement all Confidential information in tangible or electronic form under the control of the Recipient shall either be destroyed, erased or returned to the Discloser promptly upon the earlier of: (i) the written request of the Discloser, or, (ii) termination or expiry of this Agreement or, in respect of the SLAs, the termination or expiry of the SLAs. Notwithstanding the forgoing, both Parties may retain, subject to the terms of this Agreement, reasonable number of copies of the other Party's Confidential Information solely for confirmation of compliance with the applicable laws and recipient shall promptly notify the retention of such documents with the purpose so specified to the Discloser. .
- n. Neither Party is restricted by the provisions of this clause from using (including using to provide products or perform services on behalf of third Parties) any ideas, concepts, know-how and techniques that are related to the Recipient's employees or agents (and not intentionally memorized for the purpose of later recording or use) (collectively, the "residuals"). This Article shall not permit the disclosure or use by either Party or any financial (including business plans), statistical, product, personnel or customer data or the other Party. Each party agrees not to disclose the source of the Residuals.
- o. Receiving Party agrees that monetary damages would not be a sufficient remedy for any breach of this clause by the Receiving Party and that VSCDL, as appropriate, shall be entitled to equitable relief, including injunction & specific performance as a remedy for any such breach. Such remedies shall not be deemed to be the exclusive remedies for a breach by a Party of this clause, but shall be in addition to all other remedies available at law or equity to the damaged Party.

5. Term

Upon signature by both the parties, this Agreement shall come into effect from the Effective Date (which is the date of contract signing between FIRST PARTY and SECOND PARTY) and shall continue in full force for perpetuity, in relation to the Purpose, which includes obligations relating to the protection of the confidential information. The violation of confidentiality and disclosure in violation of all conditions of Para 4 above will prime to action under relevant statutory provisions.

6. No License

No license or conveyance of any rights held by First Party under any discoveries, inventions, patents, trade secrets, copyrights, or other form of intellectual property is granted or implied by this Agreement or by the disclosure of any Confidential Information pursuant to this Agreement.

7. Severability

In the event that any of the provisions contained in this Agreement is found to be invalid, illegal or unenforceable in any respect by a Court of competent jurisdiction, the validity, legality, or enforceability

of the remaining provisions contained in this agreement will not be in any way affected or impaired by such a finding.

8. General

- p. **Amendment:** No delay by disclosing party in enforcing any of the terms or conditions of this Agreement shall affect or restrict Disclosing Party's rights and powers arising under this Agreement. No amendment of any term or condition of this Agreement will be effective unless made in writing and signed by both parties.
- q. **Relationship:** The Parties to this Agreement are independent contractors. Neither Party is an agent, representative, or partner of the other Party. Neither Party shall have any right, power, or authority to enter into any agreement for, or on behalf of, or incur any obligation or liability of, or to otherwise bind, the other Party. No joint venture, partnership or agency relationship exists between the First Party or Second Party or any third-party as a result of this Agreement.
- r. **Assignment:** Neither Party may assign its rights or delegate its duties under this Agreement without the other Party's prior written consent.
- s. **Waiver:** Neither Party will be charged with any waiver of any provision of this Agreement, unless such waiver is evidenced by a writing signed by the Party and any such waiver will be limited to the terms of such writing
- t. **Entire Agreement:** This Agreement forms the entire agreement between the parties relating to Confidential Information disclosed in connection with the Purpose and it replaces and supersedes any previous proposals, correspondence, understandings or other communications whether written or oral relating to the subject matter hereof.
- u. **Severability:** If any provision of this Agreement is determined to be invalid in whole or in part, the remaining provisions shall continue in full force and effect as if this Agreement had been executed without the invalid provision illegal or unenforceable parts had not been included in this Agreement.
- v. **No Publicity:** No press release, advertisement, marketing materials or other releases for public consumption concerning or otherwise referring to the terms, conditions or existence of this Agreement shall be published by the Second Party. The Second Party shall not promote or otherwise disclose the existence of the relationship between the Parties evidenced by this Agreement or any other agreement between the Parties for purposes of soliciting or procuring sales, clients, investors or other business engagements without approval of First Party.
- w. Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the Parties, their successors and assigns;

9. Governing law and jurisdiction

This Agreement is governed by and shall be construed in accordance with the laws of India. In the event of dispute, the parties shall attempt to resolve the dispute in good faith by senior level negotiations. In case, any such difference or dispute is not amicably resolved within forty-five (45) days of such referral for negotiations, it shall be resolved through arbitration, in India, in accordance with the Arbitration and Conciliation Act, 1996. The venue of arbitration in India shall be Vadodara.

Subject to the foregoing provisions on alternative dispute resolution, the competent courts of Vadodara shall have the exclusive jurisdiction in connection with this Agreement. Any claim for damages under this Agreement shall be restricted to direct damages only.

The parties have caused this Agreement to be executed by their duly authorized representatives and made effective from the Effective Date first written above.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their duly authorized representatives and made effective from the Effective Date first written above.

<p>SIGNED for and on behalf of</p> <p>_____</p> <p>By _____</p> <p>Title _____(authorized signatory)</p> <p>Date _____</p>	<p>SIGNED for and on behalf of</p> <p>_____</p> <p>By _____</p> <p>Title _____(authorized signatory)</p> <p>Date _____</p>
--	--

Witness 1 :

Name :

Address:

Designated as :

Ph:

Witness 2:

Name :

Address:

Designated as :

Ph: