



National Forensic Sciences University

Knowledge | Wisdom | Fulfilment

An Institution of National Importance
(Ministry of Home Affairs, Government of India)

Expression of Interest (EOI)

Empanelment of Vendors for Providing Managed Next Generation Security Operations Centre (NG-SOC) Services

Ref. No.: PUR/CoE- CS-1/NG-SOC Services
(1)/25-26

Centre of Excellence in Cyber Security (CoE-CS)
National Forensic Sciences University (NFSU),
Gandhinagar
Gujarat - 382007, India



Table of Contents

Section-I GENERAL INSTRUCTIONS FOR BIDDERS	3
Section-II MANDATORY QUALIFICATION CRITERIA.....	5
Section-III BUSINESS REQUIREMENTS	12
3.1 Tender Purpose: Empanelment	12
3.2 Business Functional Requirements	12
3.3 Scope of Work:.....	15
Section -IV Technical Evaluation.....	26
Section-V Technical Specifications	29
ANNEXURE - 1 Undertaking with respect to Compliance of Restrictions for Countries which share land border with India - as stipulated by Govt. of India.....	54
ANNEXURE - 2: NO BLACKLIST DECLARATION	56
ANNEXURE - 3 MALICIOUS CODE CERTIFICATE.....	57
ANNEXURE - 4 Acceptance Of Terms & Conditions of Tender Undertaking.....	58
ANNEXURE - 5 -EMD/Bid Security Form.....	59

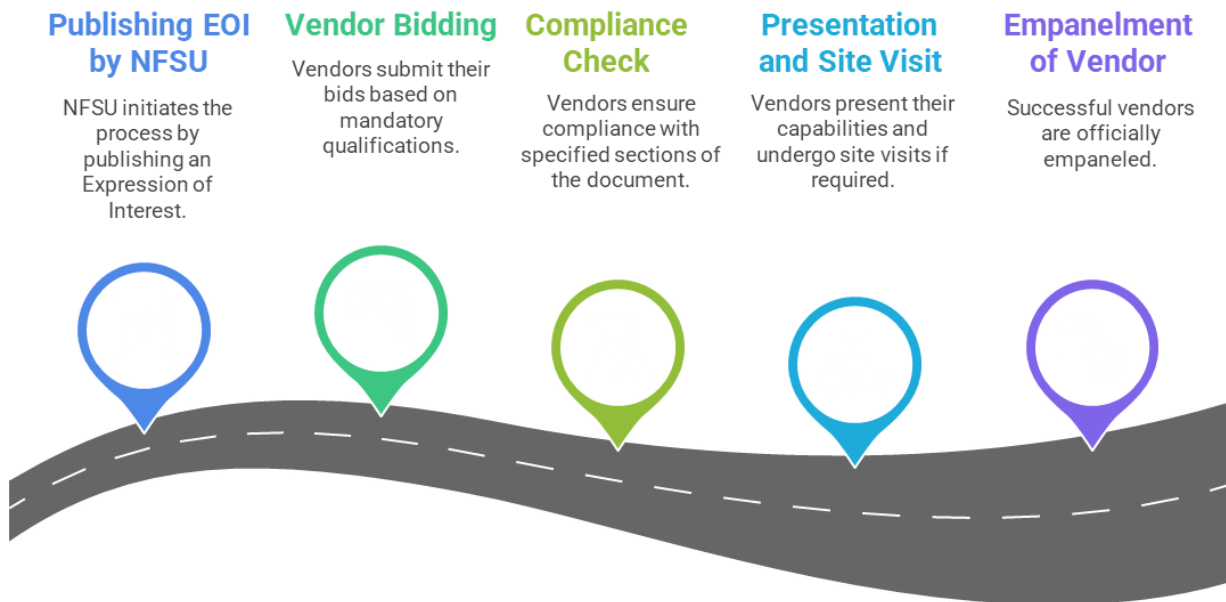
Section-I GENERAL INSTRUCTIONS FOR BIDDERS

- 1.1 National Forensic Sciences University, an Institution of National importance, having its headquarters at Sector-9, Gandhinagar-382007, Gujarat is established by an Act passed in the year 2020 by the parliament of India, to facilitate and promote studies and research and to achieve excellence in the field of forensics science in conjunction with applied behavioral science studies, law, criminology and other allied behavioral science studies, law, criminology and other related field, and to provide for matters connected therewith or incidental thereto. NFSU primarily facilitate and promote academic learning and practices in the field of forensic sciences in conjugation with applied behavioral science studies, law, legal studies, criminology and other allied areas and technology, including training skill-development, research and extension of work with focus on emerging areas in the said field for strengthening criminal justice institution in the country. At present NFSU has a total of 13 campuses within the country and one campus outside the country at Uganda. CoE-CS at NFSU is dedicated center for Cyber security and related tools and technologies. CoE-CS, NFSU has been approached by multiple clients to establish & Manage SOC for their premises.
- 1.2 Through this EOI National Forensic Sciences University (NFSU) invites proposals from reputed and experienced service providers for empanelment for a period of **05 (Five) Years** to provide comprehensive managed services for a state-of-the-art Security Operations Center (SOC). The selected vendors will work under the direction of Center of Excellence in Cyber Security (CoE-CS) of NFSU to establish, operate, and evolve SOC capabilities for NFSU or its clients.
- 1.3 The CoE-CS, NFSU reserved the right to empanel more than one bidder.
- 1.4 The CoE-CS reserves the right to reject any or all EOIs or cancel/withdraw the request inviting proposal without assigning any reason whatsoever and in such case no intending bidder shall have any claim arising out of such action.
- 1.5 This document does not constitute nor should it be interpreted as an offer or invitation for the selection of a Managed Service provider of SOC for NFSU described herein. The document will be used to empanel suitable and capable vendors for providing SOC services to NFSU and its clients.
- 1.6 This document does not purport to be all-inclusive or contain all the information or be the basis of any contract. No representation or warranty, expressed or implied, is or will be made as to the reliability, accuracy or the completeness of any of the information contained herein.
- 1.7 After the Empanelment is done, NFSU will provide the architecture of the client and already implemented tools and technology of the client to all the empaneled vendors and Afterwards after a budgetary quotation will be asked from all the vendors. The vendor providing the lowest quotation for the provided details of the client will be awarded with SOC management

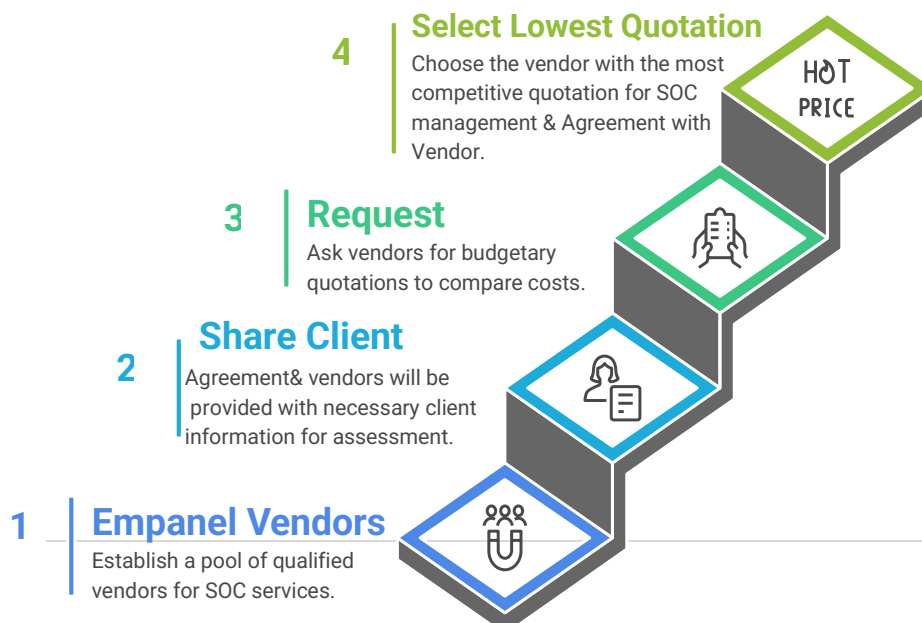
for that client. A separate agreement will be done with the bidder before the client data is shared. The agreement will include the PBG, tiebreaker rules and terms and conditions of the SOC services, for each client, a separate agreement will be done between NFSU & Bidder.

- 1.8 Officials of NFSU holds rights to visit vendor premises and can ask for presentation to understand more about the services provided by the vendor.
- 1.9 NFSU holds the rights to contact the Vendors client in order to understand the quality of service provided by the vendor
- 1.10 For further clarification, please contact: coe.cs@nfsu.ac.in, purchase_gnr@nfsu.ac.in

SOC Empanelment Process



After Empanelment Process



Section-II MANDATORY QUALIFICATION CRITERIA

Sr.	Pre-Qualification (PQ) Criteria	Document(s) to be submitted
1.	Power of Attorney (POA) in favour of the Authorized Signatory signing the bid or Board Resolution in favour of the person granting the POA (on Non-Judicial stamp paper of INR 100/- or such equivalent amount and document duly notarized). All pages of the bid document and relevant documents should be duly signed by the authorized signatory failing which the bid will stand rejected.	Power of Attorney (PoA) duly notarized to show authorization of the person Or, Board resolution copy.
2.	A bidder with solutions developed in an entity incorporated in a country sharing a land boundary with India cannot participate in this bid. (The bidder is required to submit an undertaking with respect to Compliance of Restrictions for Countries which share land border with India {Restrictions under Rule 144(xi) of the General Financial Rules, 2017. Reference OM no. 6/18/2019-PPD dtd. 23.07.2020 (read along with any subsequent clarifications/amendments thereof) issued by Ministry of Finance, Public Procurement Division (https://doe.gov.in/procurement-policy-divisions)	Land Border Undertaking (Annexure 1) duly signed and stamped by Authorized Signatory has to be submitted at the time of bid submission.
3.	The bidder should be an established Company registered under the Indian Companies Act, 1956/ 2013, or partnership firm register under LLP Act, 2008 since last 5 years as of Bid Publishing Date.	Following certificates would be required: Certificate of the incorporation, provided by Ministry of Corporate Affairs, GoI. Certificate consequent to change of name, if applicable.
4.	The bidder should have a registered number of: GST Registration. Income Tax / PAN.	Following certificates would be required: Certificate of GST registration. Copy of PAN / Income tax number.

5.	<p>The bidder should be an authorized System Integrator (SI) / Business Partner (BP) of the OEM whose product bidder is proposing for the managed NG-SOC service. OEM should not declare End of Support/life for the technology/equipment being proposed for NG-SOC at least 3 (three) years or till the extended contract date from bid closing date.</p>	<p>In case the bidder is System Integrator (SI) / Business Partner (BP) authorized by OEM then bidder need to submit a valid Manufacturers Authorization Form (MAF) (Tender specific) on the OEM Letterhead with duly stamped with valid digital/wet signature by authorized signatory of OEM's as well as acknowledged by SI / BP towards acceptance of the same on each solution / equipment must be furnished in original. SI/BP need to keep the authorization valid till execution of support period.</p> <p>Undertaking from the OEM mentioning a clause that OEM would not declare End of Support/life for at least 3 years for each solution / equipment being proposed for the managed NG-SOC service on the OEM Letterhead with duly stamped with valid digital/wet signature by authorized signatory of OEM's and must be furnished in original.</p>
6.	<p>The bidder should have a minimum annual turnover of at least Rs. 5 Crores in the last three audited financial years as on bid submission date.</p> <p>(Turnover of Rs 5 Cr can be generated from Services provided by the bidder in areas similar to Cyber Security, VAPT, SOC services, Digital Forensics, IT infra management, Data Centre Management and similar IT services)</p> <p>Note: Turnover should be applicable to bidder and not for its group companies/ subsidiary companies/ parent company</p>	<p>Audited Balance Sheets for last 3 years, i.e., 2022-23, 2023-24 & 2024-25</p> <p>where financial turnover from SOC business should be clearly mentioned. Every sheet should be duly certified by a chartered accountant or accounting firm stating Net Worth, Turnover and Profit/Loss for last 3 financial years.</p> <p>OR</p> <p>A letter under the head of the chartered accountant / or firm certifying the financial turnover of the company is to be submitted with the bid.</p>
7.	<p>Bidder should be a net profit-making organization in each of the last Five (05) financial years as on bid submission date.</p>	<p>Audited Balance Sheets for last 5 years, i.e., .2020-21, 2021-22, 2022-23, 2023-24 & 2024-25</p> <p>where profit or loss from similar works is segregated. Every sheet should be duly certified by a chartered accountant or accounting firm stating Net Worth, Turnover and Profit/Loss for last 5 financial years.</p>

		<p>OR</p> <p>A letter under the head of the chartered accountant / or firm certifying the profit and loss of the company from similar line of service is to be submitted with the bid.</p>
8.	<p>At least three (3) Central Government / State Government/ PSU/ BFSI clients shall be served by bidder, with similar nature of work (On-Premises SOC, Managed SOC, Hybrid SOC) the recent past and all work orders / contracts should be in the name of the bidder for the SOC services.</p> <ul style="list-style-type: none"> • Minimum value of any one project should be above 1 Crores or more. • One of the projects should be completed or under steady state of operations 	<p>Relevant MSA copy/ Work order copy / Customer Satisfaction Letter regarding successful implementation or ongoing implementation of security operation center (SOC) in the name of the bidder is to be submitted.</p> <p>The PO / letter should be in the name of the bidder and clearly mention the scope of work.</p>
9.	<p>The bidder should have experience of owning and managing 24x7 manned well-established Next Generation Security Operations Centre (NG-SOC) setup (India hosted). The bidder shall provide the details of the NG-SOC, including the location, infrastructure, tools used, process and methodology.</p> <p>AND</p> <p>The bidder should have at least 15 to 20 Information Technology/ Information Security/ Cyber Security Full-time Technical Support (FTS) professionals on NG-SOC service solutions / equipment's in its permanent role with expertise in:</p> <ul style="list-style-type: none"> • 24x7 Threat Monitoring & Protection • SIEM & SOAR Professionals • Manage, detect and respond to network and cyber security threats • Proactive and reactive incident response services • Security/Threat Intelligence Services • VAPT • Cyber Security Audit and Compliance • Incident Response Management. 	<p>Documentary evidence which shows that it is audited by the third party or must comply Meity / STQC guideline</p> <p>OR</p> <p>Self-Declaration in this regard with all information including the location, infrastructure, tools used, process and methodology in bidder's letterhead duly stamped with valid digital/wet signature by authorised signatory. In addition, pictures/ video footage of the established SOC facility (within Gujarat if needed), could be shared along with the technical bid.</p> <p>AND</p> <p>Manpower: Undertaking from Bidder indicating the number of certified full-time Technical Support (FTS) professionals mentioning the name & official email id in its permanent role (We may ask for educational</p>

		qualifications including certifications of the provided FTS, if required).
10.	The bidder should have a 24x7 well-established Next Generation Security Operations Centre (NG-SOC) setup at Gujarat, State of India.	Self-certification with the addresses to be submitted/ declaration for the established managed SOC. The document should be on the bidder's letter head signed by the authorized signatory. (If needed the committee may visit the SOC Center for the assessment)
11.	The bidder must own and operate a 24x7 manned, well-established Next- Generation Security Operations Center (NG-SOC). The NG-SOC should utilize the following compliance/standards for Data Centers (DCs), : <ul style="list-style-type: none"> • ISO 27001:2013/2022 • ISO/IEC 9001:2015 (if applicable) 	Self-certification with the addresses to be submitted/ declaration for the established SOC Data Center.
12.	The bidder or any of its group / sister concern company should not have been blacklisted by any Regulatory or Government Authority or Public-Sector Undertaking or any Law Enforcement Authority for breach of any Regulations or Laws as on date of submission of the tender. The bidder or any of its group / sister concern company must not have been blacklisted by any Central/ State Government Department/ PSU/ PSU Banks/ Autonomous Bodies/ Statutory Bodies or institution/ any regulator in India as of the bid submission date.	A Self certified letter (Annexure 2) by the authorized signatory of the bidder clearly stating that the bidder has not been blacklisted must be submitted on the original letterhead of the bidder with signature and stamp.
13.	The bidder should be certified to the following standards (preferably latest one): ISO 27001: 2013/ 2022 ISO 9001: 2008/ 2015 (if applicable) ISO 20000: 2018 (if applicable) SOC2 or SOC3 (if applicable)	Copy of the certificate(s) to be submitted along with the bid.

14.	The offered NG-SOC service shall follow the MeitY's data localization guidelines . The service offered shall be from Next Generation Security Operation Centre located in India . All the data collected as part of the service shall be stored within India .	Self-Declaration in this regard with location information in bidder's letterhead duly stamped with valid digital/wet signature by authorized signatory .
15.	The bidder should have an operational Disaster Recovery site hosted in India, along with an approved Business Continuity Plan to ensure uninterrupted NG-SOC service operations for client. Bidder must be empaneled with a nationally recognised institute or organisation	Business Continuity Plan. and, Self-Declaration in this regard in bidder's letterhead duly stamped with valid digital/wet signature by authorised signatory .
16.	All the software / solutions proposed for NG-SOC should be supported by a "Malicious code free" Declaration. Any upgrade/update of patches of the proposed NG-SOC software / solutions should be malicious free during the subscription period.	MALICIOUS CODE CERTIFICATE (Annexure 3) from bidder's & each OEM's letterhead duly stamped with valid digital/wet signature by authorized signatory .
17.	The bidder shall not assign or subcontract the assignment or any part thereof to any other person/firm.	Self-Declaration in this regard in bidder's letterhead duly stamped with valid digital/wet signature by authorized signatory .
18.	MSE & Startups	No Exemption & relaxation to MSE & Startups
19.	Acceptance of the terms and conditions of this EOI	Annexure 4 - Duly sealed and signed certificate on Company/Firm's Letterhead

Note:

1. Since this is not a Request for Proposal (RFP), commercials are not required to be submitted at this stage.
2. Empanelment will be for next **05 (Five) years from the date of awarding the empanelment**, the same can extended further **01 (One) to 03 (Three) years** if found suitable with further approval from the competent authority subject to satisfactory performance and reviews.
3. NFSU reserves the right to **terminate the empanelment of any bidder** at any stage if it is found that the bidder has submitted **false or misleading documents**, even after the empanelment has been awarded. Furthermore, if the services rendered by the bidder are **not in accordance with the requirements** and terms specified in this EOI, NFSU reserves the right to **cancel the bidder's empanelment without prior notice** and without assigning any reason, NFSU holds the right to blacklist the party.

PROFILE OF THE BIDDER & Technical Requirements

Sr. No.	Particulars	Response
1.	Name of the bidder	
2.	Country of HQ (if other than India) and Date of Incorporation	
3.	Head Quarters Address	
4.	Address in India & Date of Incorporation in India	
5.	Communication Details of Contact Official(s) - Name, Designation, Phone & Fax Number (with STD code), Mobile No. & E-mail Address.	
6.	Ownership structure (e.g. Company, Partnership)	
7.	Details of Partners / Directors	
8.	In case of limited companies, names of major shareholders with percentage holding.	
9.	Total number of offices worldwide and list thereof	
10.	Experience in Security Operations Centre setup & management (No of years with details of significant work done including volumes, capacities etc.)	
11.	Experience in implementing Security products (No. of years with details of products and implementation locations)	
12.	a. Total Number of Employees.	
	b. Total Number of Technical employees	
	c. Number of employees having Qualifications / Certifications (GSOC technologies proposed, CISSP, CEH, ISACA CRISC, CVA, CCNA, CCNE, CCSP, CCIE-Network, CCIE- Security etc.). (breakup of each to be given)	
13	a. Tangible Net Worth, Total turnover for the last 03 Financial Years, Sales & Profit for the last 05 Financial Years (A letter under the head of the chartered accountant / or firm certifying the profit and loss of the company from similar line of service is to be submitted with the bid)	
	b. Turnover relating to Security Operations Centre services for the last three financial years. (A letter under the head of the chartered accountant / or firm certifying the profit and loss of the company from SOC service is to be submitted with the bid)	

Sr. No.	Particulars	Response
14.	Name of Primary Bankers/Financers & their address	
15.	Furnish information relating to the Clients where security operations have been undertaken.	
16.	Furnish details of pending/past litigations within the last 3 years, if any.	
17.	Brief Bio-data of the key personnel to be associated with the proposed project	
18.	Activities proposed to be covered under Next- Gen SOC along with names of products / appliances/ solutions proposed for each activity, name & details of Partner companies / Applicants (please attach details of the arrangements).	
19.	Names of proprietary products, technologies for Security Operations Centre, used by you.	
20.	Details of empanelment / tie-ups / assignments with Government units and industry bodies	
21.	Compliance to all the technical specification as mentioned in Section III & V of this document.	

Note

The bidder must attach appropriate document attested by their Authorized Signatory in support of their claim in compliance of the above particulars

Section-III BUSINESS REQUIREMENTS

3.1 Tender Purpose: Empanelment

The Center of Excellence in Cyber Security, National Forensic Sciences University would like to empanel vendors for following purpose,

- a) Procurement of Tools, its Deployment, Integration & Implementation for SOC including its Real Time Monitoring and SOC Services along with qualified & skilled manpower as mentioned in Section 3.3.5 for NFSU or its client.
- b) Deployment & Implementation of SOC including its Real Time Monitoring and SOC Services along with skilled manpower as mentioned in Section 3.3.5 for NFSU or its client.
- c) SOC Services along with skilled manpower for monitoring of services as mentioned in Section 3.3.5 for NFSU or its client.
- d) Vulnerability Assessment and Penetration Testing Services for NFSU or its client
- e) Cyber Security Audit and Compliance Services for NFSU or its client.
- f) Incident Response Management Services for NFSU or its client.

The Managed NG-SOC Service Vendor must possess prior experience in the deployment and management of Security Operation Centers and will be responsible for below but not limited to:

- a) 24x7 Threat Monitoring and Protection
- b) Real-time Log Analysis and Security Event Correlation
- c) Managing, Detecting, and Responding to Network and Cybersecurity Threats
- d) Proactive and Reactive Incident Response Services
- e) Security/Threat Intelligence Feeds & Services
- f) Zero Day Attacks

The technical architecture including the list of components will be shared with the vendor upon empanelment.

The vendor must also ensure compliance to the regulatory compliance of NCIIPC, CERT-In, Ministry directives, and the guidelines & actionable points promogulated by NFSU.

Joint bids will not be accepted.

This bid aims to identify a qualified Managed NG-SOC Service Vendor who can effectively strengthen cybersecurity posture and meet the evolving requirements laid by NFSU or its client.

3.2 Business Functional Requirements

The proposed NG-SOC must comply with following business/functional requirements:

The bidder should provide a fully managed Next Generation Security Operation Center (NG- SOC) service that delivers continuous 24x7 security operations and monitoring.

The vendor should be able to bind to any of the following options as and when required:

- a) Procurement of Tools, its Deployment, Integration & Implementation for SOC including its Real Time Monitoring and SOC Services along with qualified & skilled manpower as mentioned in Section 3.3.5 for NFSU or its client.
- b) Deployment & Implementation of SOC including its Real Time Monitoring and SOC Services along with skilled manpower as mentioned in Section 3.3.5 for NFSU or its client.
- c) SOC Services along with skilled manpower for monitoring of services as mentioned in Section 3.3.5 for NFSU or its client.
- d) Additional services, as and when required, needs to be provided by the Vendor
 - I. Vulnerability Assessment and Penetration Testing Services for NFSU or its client.
 - II. Cyber Security Audit and Compliance Services for NFSU or its client.
 - III. Incident Response Management Services for NFSU or its client.

The vendor must also ensure:

- The bidder should ensure that the NG-SOC service is capable of monitoring and protecting both internal network traffic within client and internet traffic from all locations.
- The bidder should ensure that the solution is scalable and adaptable to changing business requirements over the contract period.
- The bidder's should ensure minimal disruption to client's ongoing operations during the deployment and transition phases.
- In case of existing SOC infrastructure: The bidder should manage all necessary licensing and subscriptions for the NG-SOC services and associated security solutions during the contract period.
- The bidder should ensure timely renewals and compliance with all licensing requirements for security tools and platforms integrated with the NG-SOC service.
- The bidder should provide 24x7 threat monitoring and protection for the entire network and IT assets.
- The bidder should conduct real-time log analysis and security event correlation to identify potential security threats.
- The bidder should manage, detect, and respond to network and cybersecurity threats across client's IT infrastructure.
- The bidder should provide proactive and reactive incident response services to mitigate security incidents promptly.
- The bidder should offer security and threat intelligence services to identify emerging threats.

- The bidder should be able to utilize open-source intelligence (OSINT) to enhance threat detection and response if required.
- The bidder should have capabilities to handle zero-day attacks and advanced persistent threats (APT).
- The bidder should be able to implement and integrate the Managed NG-SOC service seamlessly with client's existing cybersecurity infrastructure but not limited to, including firewalls, XDR, centralized monitoring systems, and other security measures.
- The bidder should ensure that the NG-SOC service is designed to integrate with client's strategic roadmap for advanced security technologies but not limited to, such as Zero Trust Security Edge (ZTSE), DDoS protection, DNS security, and Data Loss Prevention (DLP).
- The bidder should ensure that the Managed NG-SOC service is capable of adapting to future security technologies and advanced security measures as they are rolled out within client.
- The bidder should meet agreed-upon SLAs provide by NFSU or its client for security monitoring, threat detection, and incident response times.
- The bidder should adhere the SLAs for each service component provided under the Managed NG-SOC service, including response and resolution times for different threat categories as mentioned in the bid document.
- The bidder should ensure compliance with all relevant regulatory guidelines and advisories issued by regulatory bodies such as NCIIPC, CERT-In, Ministry directives, and internal requirements of NFSU & the client on time-to-time basis.
- The bidder should integrate the security/threat intelligence feed issued by regulatory bodies such as NCIIPC, CERT-In, etc., into the NG-SOC service.
- The bidder should provide continuous improvement plans and enhancements to the NG-SOC service to adapt to new cybersecurity challenges.
- The bidder should conduct regular security assessments, audits, and reviews to ensure the efficacy of the security operations.
- The bidder should provide comprehensive documentation detailing the scope, implementation, integration, customization, and maintenance of the NG-SOC services during the contract period after the empanelment and on awarding a client.
- The bidder should offer bare minimum training to client's internal security teams to ensure they can effectively collaborate with the Managed NG-SOC service team.
- The bidder should provide ongoing support and guidance to client in the event of security incidents or the need for advanced security measures.
- The bidder should implement continuous monitoring, performance auditing, and regular security reviews of the NG-SOC service to ensure it is functioning optimally.
- The bidder should have procedures in place for auditing security operations and reporting performance against defined SLAs and security metrics which

will be provided after empanelment based on NFSU or its client's requirements.

- The solution must enable continuous discovery, inventory, and risk analysis of client's digital assets, including but not limited to internet-facing IPs, domains, and applications.
- The bidder should ensure the ASM solution identifies vulnerabilities, misconfigurations, and shadow IT assets, delivering prioritized remediation recommendations. The platform should integrate seamlessly with existing security tools and provide detailed dashboards and periodic reports to facilitate informed decision-making.

3.3 Scope of Work:

The detailed scope of work in connection to establishment of Next Generation Security Operations Center (NG-SOC) services is as mentioned herewith, but may change depending on requirements from NFSU or its client on time-to-time basis. NFSU's seeks your expression of interest to enhance its client's cybersecurity framework by engaging a vendor as Managed Security Service Provider (MSSP) for the Next Generation Security Operations Center (NG-SOC) services or any of those mentioned in 3.2.

The primary objective is to establish a comprehensive and proactive security mechanism for monitoring, detecting, and responding to cybersecurity threats, thereby minimizing the risks of attacks and data breaches while ensuring compliance with regulatory requirements.

- 3.3.1 The solution provided by vendor should encompass complete managed services for a Security Operations Center, including the procurement (if required), setup, configuration, integration, and seamless operation of all required software, licenses, and resources. It must include robust capabilities like Security Information and Event Management (SIEM), Machine Learning (ML) algorithms, Artificial Intelligence (AI), Security Orchestration, Automation and Response (SOAR), advanced defense mechanisms, and reliable threat intelligence. The solution should facilitate data analytics, user behaviour analytics, and proactive threat hunting, with the ability to collect and analyze logs from endpoints, servers, the existing XDR, network, applications, and platforms like O365.
- 3.3.2 The solution provided by vendor should integrate effortlessly with client's existing and future IT infrastructure, including current and planned security solutions. It should align with client's operational requirements, existing security portfolio, and strategic objectives.
- 3.3.3 The solution provided by vendor is expected to operate **entirely within India**, with the necessary infrastructure to provide round-the-clock remote support and services for at least a three-year period. The service provider must ensure full compliance with data localization requirements by MeitY, including a

declaration that client's log data will remain within Indian borders under all circumstances.

3.3.4 The vendor should deliver a comprehensive suite of services to meet the client's requirements, including but not limited to the following components and technologies:

- Security Analytics - SIEM
- Automation and Response - SOAR
- SOC Infrastructure Setup
- Application & API Security
- Network-Based Anomaly Detection
- Database Activity Monitoring
- Privileged Access Management
- Endpoint Protection Solution
- End-point Detection and Response
- Integration with the existing IT Infrastructure
- Threat Intelligence and Threat Hunting
- MITRE ATT&CK Mapping
- Vulnerability Assessment and Prioritization
- Sandboxing
- Risk Visibility – User, Device, and Application
- Attack Surface Risk Management – Internal and External
- Portals, Reports, and Dashboards

3.3.5 The solution provided by vendor should adhere to regulatory standards, including CERT-In, NCIIPC, and other Indian regulatory bodies. The service provider should also maintain a fully functional technical support center within India.

3.3.6 The solution provided by vendor should adopt a layered security approach, with capabilities to correlate data across endpoints, servers, networks, hybrid cloud, and on- premises environments. The service must ensure that its components individually and collectively fulfill the technical requirements outlined by the client, supporting any necessary third-party hardware, software, or services to achieve the desired outcomes.

3.3.7 The solution provided by vendor is expected to maintain a high availability rate, with uptime exceeding 99.95%. It should follow globally recognized standards such as ISO / IEC & NIST.

3.3.8 The solution provided by vendor must ensure all integrated components comply with TLS 1.2 or higher from the outset. It should comply with client's Cyber Security Policy, IT Policy, and Indian regulatory standards. The service provider must proactively study, implement, and maintain any evolving regulatory or industry standards as required.

3.3.9 The solution provided by vendor should facilitate client's unrestricted use of software licenses across any number of locations. Additionally, all tools should be transferable between locations as needed. Integration APIs, connectors, and

- parsers must be shared to allow seamless integration with existing and future solutions, whether on-premises or cloud- based.
- 3.3.10 The solution provided by vendor should retain collected data online for three months, with archived data accessible for six months. Archived data must be restorable and provided to NFSU & client in formats like JSON, XML, Syslog, or CSV as required.
- 3.3.11 The vendor should deploy endpoint agents centrally using client's existing tools if available, providing all necessary scripts or files to facilitate deployment.
- 3.3.12 The vendors will be empaneled based on their willingness for providing Services and support for offered solutions and services for a period of 3 years from the date of issue of order.
- 3.3.13 The selected vendors shall deliver comprehensive services to NFSU & it's client as and when stated. This includes the provision of all necessary software, virtualization packages, operating systems compatible with client existing hypervisor, databases, and other components required to configure the log collector. The scope covers the entire lifecycle of the solution, from installation, integration with client's existing infrastructure, commissioning, and acceptance, to training, maintenance, audit compliance, and knowledge transfer, as outlined in the bid document.
- 3.3.14 The solution provided by vendor must include the following:
- Required Components: All necessary elements, such as virtualization software, operating systems databases, etc... required for the successful installation, commissioning, and operationalization of the proposed solution.
 - Licensing: Appropriate and valid enterprise-class licenses are issued in Client's/NFSU name. These licenses can be perpetual or subscription-based, as applicable.
 - Documentation: Comprehensive administrative and implementation guides provided by the respective OEMs for all components of the proposed solution.
 - Manpower: Skilled Manpower support for all levels of monitoring 24x7.
- 3.3.15 If the service provider omits any software, peripherals, or equipment necessary for the solution's successful deployment and operation, they will be required to supply such components at no additional cost to NFSU or its client.
- 3.3.16 The solution provided by vendor must ensure minimal impact on client's infrastructure, including servers, databases, endpoints, and networks, during both the implementation and operational phases of the contract. The solution must also be implemented without causing any service disruptions throughout its lifecycle.
- 3.3.17 Additionally, all components (software and hardware) provided as part of the solution must be of the latest versions. The components offered should not reach their End of Life (EOL) within the next three years to ensure long-term compatibility and support.

- 3.3.18 The vendor shall be responsible for continuously monitoring and analyzing security events across servers, databases, networks, endpoints, applications, and other critical IT assets. The service provider shall detect and assess potential security threats, investigate incidents, and respond to security events in a timely manner. Additionally, all security findings, alerts, and incident reports shall be communicated to the CISO, the CISO team, and other relevant stakeholders to ensure effective threat mitigation and response.
- 3.3.19 The Incident Response capabilities shall include, but not be limited to, isolating affected endpoints, blocking malicious activities, and terminating unauthorized or suspicious file and process executions. The service provider shall ensure swift containment, mitigation, and remediation of security incidents in alignment with industry best practices and client's security policies.
- 3.3.20 The Threat Hunting and Incident Response capabilities shall include, but not be limited to, proactive threat detection, sweeping for indicators of compromise (IOCs), executing remote shell commands, performing memory dumps, and deploying custom scripts as required. The vendor shall also facilitate forensic analysis by leveraging appropriate tools to gather artifacts for detailed investigation and remediation, ensuring alignment with industry best practices and as per NFSU's guidelines & Client's security policies.
- 3.3.21 The Triaging and Root Cause Analysis (RCA) process shall involve assessing security incidents, analyzing their impact, and determining the underlying cause. The service provider shall conduct a detailed investigation to identify the factors contributing to the incident and recommend appropriate remediation measures. Based on the RCA findings, necessary corrective actions shall be implemented to prevent the recurrence of similar incidents, ensuring alignment with industry best practices.
- 3.3.22 The solution provided by vendor must have the capability to detect, block, quarantine, or remediate files and IT threats based on hashes, Indicators of Compromise (IOC), and Indicators of Attack (IOA) provided by CERT-In or any other recognized regulatory bodies, both domestic and international. The NG-SOC solution should achieve this through its endpoint protection mechanism and seamlessly integrate these IOC/IOA as custom threat intelligence feeds within the provided solution.
- 3.3.23 The proposed solution must provide continuous monitoring of client's attack surface, both internally and externally, utilizing the capabilities available within the offered platform. The solution should identify and assess risks associated with users, accounts, devices, vulnerabilities, and applications while providing actionable insights and recommendations for remediation.
- 3.3.24 The vendor needs to configure and optimize correlation rules using the SIEM capabilities to enhance threat detection and response.
- 3.3.25 The vendor needs to implement automation and response workflows leveraging SOAR capabilities, customized to align with client's security environment.

- 3.3.26 The vendor shall analyze and monitor detections from the Client 's Extended Detection and Response (XDR) solution, contributing to improved threat detection, reduced security breach risks, and ensuring an appropriate response to incidents.
- 3.3.27 Upon detection of new threats or IOCs within client's environment, the solution must conduct analysis to assess their presence on other protected systems, identify potentially compromised assets, and recommend appropriate remediation measures.
- 3.3.28 The vendor shall perform threat containment and response, including remediation planning and the implementation of preventive measures.
- 3.3.29 The vendor shall ensure immediate and automated response to alerts using predefined playbooks to minimize response time.
- 3.3.30 The vendor shall conduct periodic, proactive, and on-demand IOC sweeps across the environment. Perform proactive IOA/IOC hunting to detect and mitigate threats before an attacker can achieve their objective.
- 3.3.31 The solution provided by vendor must be capable of detecting, blocking, quarantining, and remediating files or IT threats based on hashes, IOCs, and IOAs released by CERT-In and other regulatory bodies in India and abroad. These IOCs/IOAs must be ingested as custom threat feeds within the solution.
- 3.3.32 The vendor shall detect malicious or abnormal activities and generate alerts for events that indicate potential security breaches.
- 3.3.33 The vendor must provide 24x7 monitoring and alerting, with L1, L2, and L3 resources, along with dedicated teams for threat hunting, threat research, malware analysis, customer experience, customer success, and incident response.
- 3.3.34 Deployed manpower should be capable enough to clearly document 'process' and 'procedures' for the operational areas like Incident Monitoring & Management, Logging & Monitoring, Storage & Backup Management, privacy management. Refer ISO 27001:2013/2022, ISO/IEC 27002 standard.
- 3.3.35 Subject Matter Experts: SME's responsible to manage additional security components like DAM, WAF etc; should not only have tool/solution management experience but also should have practical knowledge of the respective security domain (that particular tool/ solution caters).
- 3.3.36 The vendor shall include a security advisory service that provides proactive threat intelligence, including Indicator of Compromise (IOC) and Indicator of Attack (IOA) sweeping, as part of the standard service offering without additional cost.
- 3.3.37 The vendor needs to provide a dedicated dashboard that enables real-time log search, visualization, and customizable widget creation, allowing users to tailor views based on security monitoring requirements.
- 3.3.38 The service provider must ensure that all data, files, and information related to client are stored exclusively on servers located within India. No sensitive or critical information pertaining to the client may be transmitted outside India or shared with any third party under any circumstances.

- 3.3.39 The NG-SOC solution must conduct threat detection and analysis on hosted servers while ensuring that critical and sensitive data from the client is excluded from processing. This ensures the protection of client's sensitive information while maintaining an effective cybersecurity posture.
- 3.3.40 The vendor must fulfil all technical requirements which will be outlined when the agreement will be done for such tender after the empanelment process. During the contract period, any customization, configuration, enabling/disabling of features, or parameter adjustments will be managed by the service provider or the Original Equipment Manufacturer (OEM) at no additional cost to client.
- 3.3.41 Any new security solutions procured by the client during the contract period, in line with industry standards, must be smoothly integrated into the existing service framework. If additional licenses are needed, their procurement and integration will be charged as per the applicable rates.
- 3.3.42 The bidder must develop and deploy any interfaces necessary to integrate the proposed solutions with client's existing applications, infrastructure, or systems. These integrations need to be carried out. Relevant data or inputs required for such integration will be provided by NFSU or its Client.
- 3.3.43 All proposed solutions must support proxy-based internet connectivity, ensuring updates (e.g., definitions, signatures) are routed through client's proxy server. Additionally, integration with the web proxy must facilitate the implementation of web access policies based on endpoint states (e.g., suspected or infected devices) identified by the solution. The integration should also allow the blocking of Command-and-Control (C&C) communication attempts detected by the platform.
- 3.3.44 Finally, logs from all network and security devices, applications, and solutions must be forwarded to the SOC service platform for centralized monitoring and analysis.
- 3.3.45 The necessary network connectivity for the NG-SOC will be provided by NFSU or its client after the empanelment. The bidder is required to design their solution to integrate seamlessly with the provided connectivity infrastructure.
- 3.3.46 The bidder service provider must maintain robust and comprehensive documentation that details configurations, integration methods, deployment architecture, and support mechanisms. This documentation should be accessible to NFSU / Client, clearly outlining roles, responsibilities, and processes. Upon empanelment of the vendor.
- 3.3.47 The bidder will provide, prepare and submit detailed SOPs, including specific commands and guidelines for integrating monitored systems based on NFSU or its client's requirement after the empanelment. Bidder must install agents on devices located in client's data center, branches, cloud environments, and roaming endpoints. Device configurations will be performed in coordination with client or its outsourced partners.
- 3.3.48 After the empanelment and during the contract period, the bidder must provide documentation and manuals in standard or client-specific formats. These must include, but are not limited to:

- Solution architecture
 - Project plans with milestones and deliverables
 - High-Level and Low-Level Design (HLD/LLD) documents, including network architecture and traffic flow details
 - SOPs
 - Product literature and operating manuals
 - Troubleshooting guides
 - Infrastructure build documents
 - Support and escalation matrices (bidder and OEM)
- 3.3.49 After empanelment of the vendor, the proposed solutions should not necessitate significant changes to client's existing network architecture or device replacements, except under the following conditions:
- Deployment of solutions requiring in-line or passive architecture changes and traffic rerouting.
 - Port mirroring for solutions reliant on mirrored traffic.
 - Any required network changes must be documented in the implementation design document, with appropriate guidance provided to client for execution.
 - The service provider will generate and provide various reports, including but not limited to:
 - Executive Reports - Weekly, monthly
 - Incident Response Reports - Ad-hoc, Monthly
 - Infected and outdated System Reports - daily, Weekly
 - Malware/threat Reports - daily, Weekly
 - System Health Reports - daily, Weekly
 - Endpoint agent status report - daily, Weekly
 - Endpoint agent availability report - daily, Weekly
 - Other customized reports as required by NFSU / NFSU's Client
 - Reports and logs for Audit Trails.
 - Reports as per the requirements of the regulators etc.
 - Specific / custom reports will have to be provided within 01 day from the time of request raised by NFSU / NFSU's Client.
 - Periodic AUDIT / VAPT REPORTS AS APPLICABLE
- 3.3.50 The empaneled vendor will be responsible for creating and maintaining a comprehensive Management Dashboard and MIS reports that cover all relevant technologies and activities. The vendor must clearly outline all the reports that will be provided to the client related to the SOC's operations and performance. There should be no restrictions on the number of reports available for viewing or downloading by the Client.
- 3.3.51 After the empanelment, the following categories of reports are the minimum required; however, the vendor is encouraged to provide additional reports as needed to enhance visibility and security:
- Daily Reports
 - No of incidents.

- Detailed report on the most accessed firewall ports (inbound/outbound).
- Weekly Reports
 - Status update on all security incidents for the week.
 - Key Findings.
 - Monitoring Summary.
 - Incident Summary.
 - RCA for the critical incidents.
 - Threat Summary.
 - Recommendations.
 - Overall Security posture.
 - Weekly threat advisory, highlighting vulnerabilities and potential threats.
- Monthly Reports
 - Comprehensive summary of incidents and events, correlation analysis, recommendations, and updates on implemented actions.
 - Trend analysis, comparing the current month's data with previous cycles (weekly, monthly, quarterly, and yearly).
 - Executive summary covering all SOC services delivered during the month.
 - Monthly security incident status report. Total number of incidents (P1 - P4) that occur during the month. Number of incidents (P1 - P4) that meet the response criteria defined in the SLA.
 - Incidents mapping to MITRE ATT&CK Framework.
 - In-depth trend analysis of security incidents for the month.
 - Uptime report.
 - False Positive report.
 - Metrics like Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR)

3.3.52 The following represent the broad expectations regarding the OEM's role during the contract period after empanelment, with the provision that NFSU and its clients reserves the right to modify the scope as needed:

- Ensure that the proposed solution design and architecture meet the project's functional and technical requirements.
- Actively monitor and provide guidance during implementation across all designated locations to ensure the project's objectives are met.
- Provide SME assistance to the implementation teams to address technical and operational challenges effectively.
- Adapt the solution to align with NFSU / NFSU's Client 's specific requirements, ensuring seamless integration with the existing infrastructure. Customizations must meet the expectations detailed in the bid document.

3.3.53 The empaneled vendor is responsible for delivering a robust, comprehensive cybersecurity solution tailored to the needs of the clients. Vendor should meet the following requirements to ensure proactive monitoring, detection, and

response to cybersecurity threats, providing client with a secure and resilient environment:

Expertise and Certification:	The vendor must be an OEM Certified Support & Services Provider, equipped with cybersecurity professionals who possess the knowledge and skills necessary to address and mitigate evolving cyber threats.
Threat Monitoring and Analysis	Analyze and monitor detections from client existing solutions to enhance threat detection, minimize security breaches, and ensure an appropriate response to incidents. Monitor abnormal activity across servers, databases, networks, endpoints, and applications, identifying threats, investigating incidents, and providing real-time updates to the CISO/concerned teams
Holistic Security Monitoring	Detect and respond to threats across multiple security control points, including endpoints and networks, leveraging data collected across domains. Provide 24x7x365 monitoring for alerts and incidents, including logs from third-party products and in-house applications
Incident Detection and Response	Monitor, detect, prevent, and respond to known and unknown threats, including bot activity and anomalies. Deliver extended visibility, analysis, and response across endpoints, servers, networks, and identities. Create trends based on recurring incidents and provide remediation suggestions to client's IT/security team.
Threat Prioritization and Remediation	Prioritize alerts and threats based on their potential impact, escalating critical threats to high-value endpoints as required by client. Perform metadata analysis to assess the impact of new threats/IoCs across the environment and provide suitable remediation measures.
Integration and Threat Intelligence	Ensure integration with OEMs, third-party threat intelligence platforms, CERT-In, and other applicable threat sources. Handle third-party log ingestion for historical analysis, real-time alerting, and compliance reporting.
Proactive Threat Management	Conduct IOC/IOA sweeping and proactive threat hunting to prevent attackers from achieving their objectives. Periodically perform health check-ups of client's IT infrastructure and share detailed reports.
Incident Management and Root Cause Analysis (RCA)	Investigate incidents, perform RCA, and document findings along with recommendations and lessons learned. Provide containment, cleanup, and remediation measures for detected threats
Automation and Customization	Automate alert responses using playbooks and SOAR capabilities, customized to client's environment. Develop and implement correlation rules and use cases following methodologies like the Cyber Kill Chain
Regulatory Compliance	Ensure compliance with CERT-In guidelines and other regulatory requirements for threat detection, response, and reporting. Maintain log retention as per local regulatory standards and synchronize devices with NTP for accurate audit trails.
Reporting and Communication	Provide detailed reports, including weekly/monthly updates, RCA reports, SLA adherence, baseline assessments, and incident summaries. Establish strong collaboration and communication with NFSU & client's team, leveraging tools like MS Teams / Cisco WebEx
Continuous Improvement	Update and maintain baselines for all monitored platforms, ensuring the solution evolves with changing security needs. Maintain a tamper-proof evidence repository for incidents and update the knowledge base with emerging security trends

Platform and Infrastructure Monitoring	Ensure integration with client's existing ITSM tool. Monitor business applications, databases, and network behaviours for anomalies, including zero-day attacks.
Additional Responsibilities	Ensure 100% communication between endpoints and the cloud/data center, resolving agent communication issues in coordination with client. Detect, block, quarantine, and clean IT threats based on advisories from CERT-In or other regulatory bodies during the contract period without additional charges.

3.3.54 The empaneled vendor should also be able to provide dashboards including and not restricted to:

Centralized Dashboard	The vendor should offer a comprehensive dashboard that provides detailed insights into license usage, security configurations, system performance, and other critical components essential for managing the SOC environment efficiently.
Enterprise-Level Security Posture Overview	The solution must provide a unified dashboard for an overarching view of the organization's security posture. The dashboards should be customizable to suit organizational needs and include role-based access controls for administrators and other users
User-Friendly Interface	The vendor must feature a highly intuitive and visually appealing graphical user interface (GUI), ensuring ease of use for both technical and non-technical stakeholders.
Flexible Report Export Capabilities	The system should have the capability to generate and export results, reports, and other relevant data in standard formats such as CSV, PDF, and others and event can be downloaded.
Customized Dashboards for Specific Requirements	The service provider should deliver dashboards tailored to NFSU / NFSU's Client 's requirements, such as: <ul style="list-style-type: none"> • MITRE TTP-based threat analysis • Risk scoring specific to NFSU / NFSU's Client 's environment • Metrics like Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) • Real-time updates on ticket statuses and other operational parameters

3.3.55 Service Level Objectives

The vendor must bind to the below-mentioned Service Level Objectives, which may deviate after the empanelment depending upon NFSU or its client's requirement.

Sl. No.	Service Area	Service Level
1	Monitoring and Incident Alerting	Ensure ingestion and real-time monitoring of 100% logs from all client systems. Log Analysis Services 24x7 monitoring of all in-scope devices. Categorization of Incidents into Critical, High, Medium and Low priority shall be carried out in consultation with the selected bidder during the contract period. All Critical, High and Medium priority incidents should be logged as incident tickets and alerted as per SLO. <ul style="list-style-type: none"> ○ Critical incident within 60 minutes of the event identification ○ High priority incident within 90 minutes of the event identification ○ Medium priority incident within 120 minutes of the event identification ○ Low priority incident within 240 minutes of the event identification Threshold: SLO compliance $\geq 98\%$, measured per month
2	Threat Intelligence Integration	Update threat intelligence feeds every 24 hours. Threshold: SLO compliance $\geq 99\%$, measured per month
3	Vulnerability Management	Identify and prioritize 100% of critical vulnerabilities within 48 hours of discovery for Servers and Endpoint only. Threshold: SLO compliance $\geq 95\%$, measured per month
4	Proactive Threat Hunting	Conduct at least one proactive threat-hunting session per week. Threshold: SLO compliance $\geq 95\%$, measured per month
5	Reports Dashboard	Daily Reports Weekly Reports Monthly Reports Threshold: SLO compliance $\geq 98\%$, measured per month
6	Service uptime	Maintain SOC tool and platform availability at 99.5% uptime. Threshold: SLO compliance $\geq 99.5\%$, measured per month
7	False Positive Reduction	Ensure $< 5\%$ false positives in security alerts. Threshold: SLO compliance $< 5\%$, measured per month
8	Periodic Review	The SOC project manager or location delegate from the bidder is expected to conduct a monthly review meeting with NFSU / NFSU's Client 's officials resulting in a report covering details about the current SOC SLO's compliance reporting, status of operation, key threats and identified new threats, issues and challenges.
9	Ticket Response Time	P1 Response Time - < 60 Minutes P2 Response Time - < 90 Minutes P3 Response Time - < 120 Minutes P4 Response Time - < 240 Minutes Threshold: SLO compliance $\geq 95\%$ for Response Time measured per month.

Section -IV Technical Evaluation

4.1 Technical Evaluation

The University may empanel number of bidders based as per the requirements of the university, based on the highest technical score achieved by the bidder during their technical assessment. The weightage of technical bid will be calculated on total marks of technical evaluation scoring parameters.

Evaluation of bid shall be carried out in below stage process as under:

- Pre-qualification (Mandatory Qualification Criteria - Section - II) eligibility evaluation.
- Compliance to Section III & minimum technical specification as mentioned in Section V of this document.
- Technical evaluation.

The objective of this evaluation methodology is to facilitate the selection of the most optimal service provider that appropriately meet the business requirements of the NFSU or its clients. All bids shall be evaluated by a Committee set up for this purpose by NFSU.

NFSU reserves the right to accept or reject any First (Original) or Updated bid, and to annul the bidding process and reject all bids at any time prior to empanelment, without thereby incurring any liability to the affected Bidder or any obligation to inform the affected Bidder of the grounds for such action.

- Those bids which fulfil the Mandatory Qualification Criteria as specified in Section-II, Section-III and comply with technical specification as specified in Section-V, will be considered for technical score calculation as defined in Clause 4.2
- The bid evaluation committee shall prepare a comparative statement in tabular form in accordance with rules along with its report on evaluation of technical terms for acceptance to empanelment process.

4.2 Technical Evaluation

NFSU shall form an evaluation committee who shall score the bids as per the guidance below. The total technical evaluation would comprise of 100 marks with the following breakup:

Stage	Description	Maximum Score	Minimum qualifying Score
Stage A (20% weight in Technical Score)	Bidder's Qualification	20	14
Stage B (60% weight in Technical Score)	1. Technical Presentation by Bidder should focus on: (a) Company Overview and relevant experience (b) Understanding of NG-SOC (c) NG-SOC Project/s undertaken by the bidder (d) Technology Stack and tools (e) Detection and response capabilities (f) Teams and expertise (g) Innovations (h) Bidders certifications and accreditations 2. Visiting of Data center by CoE CS, NFSU team (if required)	60	42
Stage C (20% in weight in Technical Score)	Compliance with Technical Specifications as per <u>Section V</u> of this document.	20	14
	Total	100	70
	Overall Qualifying %	70%	

Any deviation from the Technical Specification should be clearly brought out. NFSU's Technical Evaluation Committee may at its discretion accept, seek further clarifications, or reject any such deviation.

Scores for the above individual parameters shall be added to determine the technical scores of the Bidders.

4.3 Termination of contract and Exit Clause

a) Termination Clause

The Purchaser reserves the right to terminate the empanelment of any vendor, in whole or in part, at any time by providing written notice, under the following conditions:

- If the empanelled vendor is found to have provided false or misleading information during the bidding or empanelment process.
- If the empanelled vendor fails to respond to requests for services or proposals within reasonable timelines, or refuses to participate in service delivery as per the scope defined in future work orders.
- If the empanelled vendor breaches any terms and conditions of the empanelment agreement or fails to comply with directions issued by the Purchaser.
- If the vendor engages in any activity that is considered to be against the interests of national security, data confidentiality, or client trust.

In such cases, the empanelment may be terminated with immediate effect, and the University reserves the right to debar the vendor from participating in any future tenders for a specified period. If any security or performance guarantee has been submitted as part of future contracts/work orders, the same may be invoked in part or in full.

Termination under this clause does not prejudice the Purchaser's right to seek compensation for any losses incurred due to the vendor's non-performance or misconduct.

b) Exit Clause

- The Purchaser reserves the right to withdraw, modify, or cancel the empanelment at any stage, in full or in part, without assigning any reason and without incurring any liability.
- Either party may terminate the empanelment arrangement by giving three (3) months' advance written notice to the other party, subject to there being no ongoing assignment or unresolved obligations. If the party does not provide three (3) months' advance written notice, NFSU holds the right to blacklist the party.
- If a vendor is already engaged through a separate work order arising out of this empanelment, the termination conditions and notice period defined in that work order or contract shall prevail for that specific engagement.
- Upon exit, the empanelled vendor shall ensure handover of all reports, logs, documentation, and credentials, if applicable, in a structured and timely manner, and shall support smooth disengagement without disruption.

Section-V Technical Specifications

5.1 Technical Specifications

The proposed solution must be able to meet the technical specification as mentioned in the table below.

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
A. General Requirements				
1	The NG-SOC service must be delivered by a qualified entity (OEM/SI/MSSP) with proven expertise in EDR/XDR/Threat Intel platforms provider and meeting the technical requirements outlined.	M	Yes	
2	The proposed NG-SOC service should focus on capabilities enabling proactive and predictive threat management. These may include advanced technologies like extended detection and response (XDR), attack surface management/User and Entity Behaviour Analytics (UEBA), identity security, AI-driven analytics (e.g., predictive attack path analysis), external attack surface management (EASM), SIEM, SOAR, vulnerability assessment and prioritization, and incident response. The SOC service must not be limited to traditional SIEM-based solutions and should demonstrate an ability to adapt to emerging cybersecurity challenges.	M	Yes	
3	The proposed NG-SOC solution deployment must be in SaaS model, based on the client's infrastructure and security requirements. The solution must guarantee a minimum availability of 99.5% and have an auto-scalable or dynamically scalable architecture to address scalability concerns effectively	M	Yes	
4	The proposed NG-SOC solution must ensure that all data storage, processing, and analytics occur strictly within India, complying with applicable data residency and sovereignty laws, including but not limited to the Information Technology Act and related guidelines. If the solution uses a SAAS deployment model, the service provider must adhere to MeitY guidelines or equivalent standards accepted in India.	M	Yes	
5	The proposed NG-SOC service must focus on SOAR capabilities considering asset tagging/criticality for automated response. Client may give approval for non-critical assets for taking response actions.	M	Yes	
6	The proposed NG-SOC service must support seamless integration and centralized management of all critical modules, including SIEM, UEBA, SOAR, through a unified management console. The integration may be achieved either through a single converged platform or via efficient interoperability	M	Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
	between best-of-breed modular components, without compromising performance, security, or usability.			
7	The proposed NG-SOC service must include Health Check, Quarterly BAS and First Responder in case of any suspected breach.	M	Yes	
8	The proposed NG-SOC service provider should ensure that their team possesses diverse skill sets, including security analysts, incident investigators, threat hunters, data scientists, threat intelligence analysts, incident responders, and specialized teams for Indicators of Compromise (IOC) collection, forensic investigations, and advanced analysis.	M	Yes	
9	The proposed NG-SOC service provider is expected to offer a platform with advanced machine learning capabilities and analytics for both structured and unstructured security and network data.	M	Yes	
10	The proposed NG-SOC service should support seamless integration with third-party solutions, including security tools, IT infrastructure, and cloud services, using industry-standard protocols (e.g., REST APIs, Syslog). The solution should provide pre-built integrations (OOB) with commonly used tools and platforms and should allow the creation of custom parsers to ensure adaptability to future integration needs."	M	Yes	
11	The proposed NG-SOC service provider should deploy a centralized log management solution at NFSU for collecting logs from various sources. While NFSU / NFSU's Client will provide the necessary virtual machines and storage for the log collector, the vendor is required to provide detailed specifications for the log collector.	M	Yes	
12	Entire communication between on-prem service logger components and the proposed NG-SOC service platform must be secured using industry-standard mechanisms such as token-based authentication, mutual TLS, or equivalent methods. The chosen authentication mechanism should ensure confidentiality, integrity, and resistance to unauthorized access.	M	Yes	
13	The proposed NG-SOC service provider must build the capacity of the SIEM solution to ensure log retention as follows: Online for three months. Offline for three months, with restoration capability within ten to fifteen days.	M	Yes	
	The proposed NG-SOC service provider should offer 24x7x365 real-time monitoring, analysis, and		Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
14	correlation of logs using advanced security analytics, threat intelligence, and threat hunting capabilities, including IOCs and other threat intelligence sources like vulnerability and incident reports.	M		
15	The proposed NG-SOC service provider must enable the establishment of capabilities for SIEM, Big Data Security Analytics, and SOAR. The solution must support indexing, searching, analysis, correlation, reporting, visualization, and orchestration of structured and semi-structured data generated within the organization. These capabilities may be delivered through an integrated platform or a combination of interoperable tools, ensuring seamless functionality and operational efficiency.	M	Yes	
16	The proposed NG-SOC service provider should ensure logs are stored using industry-standard solutions and formats.	M	Yes	
17	The proposed NG-SOC service provider must ensure that log collection agents can store logs for at least three days in case of connectivity loss with the logger and automatically forward them once connectivity is restored.	M	Yes	
18	The proposed NG-SOC service provider should implement robust alert mechanisms for events and incidents while recommending remedial actions and conducting triage to eliminate false positives.	M	Yes	
19	The proposed NG-SOC service provider should provide detailed reports, including daily event/incident correlation analysis and recommendations. Monthly reports should summarize incidents, trends, and actions, comparing current data with the previous month.	M	Yes	
20	The proposed NG-SOC service provider must incorporate machine learning and security analytics to detect both known and unknown threats, consolidating data from various intelligence sources to extract actionable insights.	M	Yes	
21	The proposed NG-SOC service provider is required to conduct proactive threat hunting daily to detect threats undetected by signature-based systems and maintain readiness to swiftly respond to cyberattacks.	M	Yes	
22	The proposed NG-SOC service provider should ensure comprehensive analysis and correlation of logs from all devices under scope, including developing parsing rules for standard and non-standard logs, with pre-defined or customized parsers available for applications like Oracle E-Business Suite and OpenText Documentum.	D	Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
23	The proposed NG-SOC service provider must provide connectors for standard devices and applications and develop customized connectors for non-standard devices as required, without additional cost.	M	Yes	
24	The proposed NG-SOC service provider should deliver 24x7x365 uninterrupted security monitoring operations, supported by automated processes to reduce resource drain and response times, including a central dashboard for real-time visibility of incidents and organizational risk posture.	M	Yes	
25	The proposed NG-SOC service provider must comply with Indian government regulations and ensure seamless integration with NFSU / NFSU's Client IT systems using standard protocols without impacting existing functionality.	M	Yes	
26	The proposed NG-SOC service provider should cooperate with audits conducted by NFSU / NFSU's Client, third parties, or regulatory bodies, ensuring prompt resolution of audit observations and preventing their recurrence. Noncompliance may attract penalties as defined in the SLA.	M	Yes	
27	The proposed NG-SOC service provider should offer a solution encompassing security monitoring, incident response, threat intelligence, proactive threat hunting, SIEM engineering, SOAR Automation, User Behavioural Anomaly Detection (UEBA)/Attack Surface Management, and network threat detection.	M	Yes	
28	The proposed NG-SOC service provider should ensure the SOC solution monitors applications and databases, correlates their logs, and develops Standard Operating Procedures (SOPs) for all services, including alert and incident management, report generation, log storage, and operational continuity.	M	Yes	
29	The proposed NG-SOC service provider must deliver analytical reports on daily, weekly, and monthly intervals, as well as ad-hoc reports as required.	M	Yes	
30	The proposed NG-SOC service provider should provide IT forensic services for root cause analysis and incident investigations as required.	M	Yes	
31	The proposed NG-SOC service provider must submit an annual SOC efficacy report using a quantifiable method outlined in the RFP.	M	Yes	
32	The proposed NG-SOC service provider should ensure that, at the end of the contract, all logs retained at their end are transferred to NFSU / NFSU's Client without additional cost.	M	Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
B. Security Monitoring Requirements				
1	The proposed NG-SOC service provider solution should proactively monitor security logs to identify abnormal or potentially malicious activities and generate alerts for any incidents that might lead to security breaches.	M	Yes	
2	The proposed NG-SOC solution must have the capability to establish and maintain log baselines across all critical platforms, systems, and applications specified in the RFP scope. The solution should support monitoring capabilities that ensure visibility, anomaly detection, and alerting based on these baselines, aligned with industry best practices.	M	Yes	
3	The proposed NG-SOC service provider solution must design to collect logs seamlessly from commonly used platforms, including Windows, Linux, AIX, firewalls, network devices, and various security devices.	M	Yes	
4	The proposed NG-SOC service provider solution should also possess the capability to gather logs from network and security devices, databases, web servers, cloud platforms like AWS and Azure, SaaS solutions, and enterprise tools like O365.	M	Yes	
5	The Proposed NG-SOC Services Provider shall be able to collect and correlate XDR activity data for one or more XDR Sensors in the scope but not limited to – endpoints, email, servers, cloud servers, and networks.	M	Yes	
6	The proposed NG-SOC service provider solution should ensure detection of both internal and external attacks while continuously monitoring security events across IT infrastructure, databases, and servers.	M	Yes	
7	The proposed NG-SOC solution should support integration with NFSU / NFSU's Client Proposed/Road Map security solutions like Database Activity Monitoring (DAM), Privileged Access Management (PAM), and Data Loss Prevention (DLP) systems via standard APIs or protocols to ensure seamless interoperability and scalability.	M	Yes	
	The proposed NG-SOC service provider solution must perform log correlation across multiple sources		Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
8	to detect complex, multi- vector attacks. Detailed mitigation steps must be shared with authorized personnel, including designated service providers of the organization.	M		
9	The proposed NG-SOC service provider solution should incorporate workflows that automate routine incident response tasks, such as managing false positives, maintaining whitelists, escalation procedures, and adherence to SLAs.	M	Yes	
10	The proposed NG-SOC service provider solution should ensure that only alerts verified through a thorough triage process are communicated to the organization. Alerts generated from SIEM systems must be enriched with contextual information, historical data, vulnerability analysis, and threat intelligence.	M	Yes	
11	The proposed NG-SOC solution must have the capability to analyze historical security metrics, including attack frequency, source analysis, and target activity, to enhance threat detection and reduce false positives. The solution should leverage advanced analytics, including AI/ML capabilities or equivalent technologies, to provide actionable insights and continuously improve the quality of alerts and threat identification.	M	Yes	
12	The proposed NG-SOC service provider solution should deliver long-term strategies and mechanisms to prevent recurring threats effectively.	M	Yes	
13	The proposed NG-SOC service provider solution should support the definition, development, and implementation of use cases based on industry-standard frameworks such as the Cyber Kill Chain.	M	Yes	
14	The proposed NG-SOC service provider solution should facilitate integration of logs from non-standard applications and devices while ensuring that these logs are processed for generating actionable alerts and detailed reports mainly CEF, LEEF and JSON format.	M	Yes	
	The proposed NG-SOC service provider solution reports should align with global best practices and		Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
15	standards like ISO 27001, PCI DSS/SOC1/SOC2, while also meeting regulatory requirements such as CERT-In, NCIIPC, and SEBI guidelines.	M		
16	The proposed NG-SOC service provider solution should support log retention policies in compliance with local regulatory requirements, including those set by the CERT- In and other relevant authorities.	M	Yes	
17	The proposed NG-SOC service provider solution should include configurable rules to detect suspicious activities based on event logs but not limited to. Examples include: Failed login attempts. Successful logins from unusual systems or locations. Unauthorized authorization attempts. Vendor logins from restricted subnets. Network scans (vertical and horizontal). Traffic originating from blacklisted IP addresses. Login attempts at unusual times.	M	Yes	
18	The proposed NG-SOC service provider solution should generate insightful charts and analytics, including top attackers, attack patterns, trending risks, and threat demographics.	M	Yes	
19	The proposed NG-SOC service provider solution must ensure detailed capture of raw logs, events, and alerts, standardizing them into formats that are easy to interpret and analyze.	M	Yes	
20	The proposed NG-SOC solution must ensure secure and tamper-evident logging mechanisms using industry-standard technologies, such as immutable storage. The system must generate alerts for any detected tampering attempts. Additionally, all log data transmissions must be encrypted using standard encryption protocols (e.g., TLS 1.2 or higher) to ensure data integrity and confidentiality.	D	Yes	
21	The proposed NG-SOC service provider solution should ensure tamper-proof logging mechanisms and alert users of any tampering attempts. Log transmissions should be encrypted to maintain data integrity.	M	Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
22	The proposed NG-SOC service provider solution should include mechanisms to detect failures in the event collection infrastructure, with prompt notifications sent to operations teams for resolution.	M	Yes	
23	The proposed NG-SOC service provider solution should enrich collected data with contextual information, such as geographic data, blacklisted IPs, threat intelligence feeds, and other custom tags. This enrichment should occur in real time at the individual event level without reliance on post-processing lookups.	M	Yes	
24	The proposed NG-SOC service provider solution should integrate seamlessly with external systems like ticketing tools, messaging platforms, and vulnerability management solutions to enhance workflow automation through an extensible plugin architecture.	M	Yes	
25	The proposed NG-SOC service provider solution should monitor and analyze internal and external threats targeting IT infrastructure, business-critical applications, and databases while identifying anomalies in user and network behaviour.	M	Yes	
26	The proposed NG-SOC service provider should monitor, detect, and address IT infrastructure events, including but not limited to : Buffer overflow attacks. Port scans and vulnerability scans. Attempts at password cracking. Malware outbreaks (e.g., worms or viruses). Creation of services/processes. Unauthorized firewall rule changes. Unapproved system access attempts. SQL injection and cross-site scripting attacks. Layer 7 web-based attacks over intranet and internet.	M	Yes	
	The proposed NG-SOC service provider should also monitor and manage business application security incidents, including but not limited to : Attempts to breach segregation of duties. Unauthorized access or modification attempts.		Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
27	Critical user account modifications, including additions or deletions. Changes in critical application roles, groups, or permissions. Adjustments to account policies or password settings. Alterations in critical application or audit parameters.	M		
28	The proposed NG-SOC service provider shall be able to collect detection logs from existing network and security devices for Detection, Analysis, Alerting, and Correlation with XDR Telemetry collected from Endpoint, Server Sensors	M	Yes	
29	The proposed NG-SOC service provider should be monitoring High fidelity alerts and automate it with all the possible response actions.	M	Yes	
30	The proposed NG-SOC service provider should be able to Triage and provide RCA of Incidents.	M	Yes	
31	The proposed NG-SOC service provider should have a dedicated War Room facility to facilitate incident response, threat analysis, and crisis management. The facility should allow customer participation when required, ensuring collaborative decision-making and effective incident handling.	D	Yes	
32	The proposed NG-SOC service provider platform has to be tightly aligned with MITRE - ATT&CK framework with the latest version	M	Yes	
33	The proposed NG-SOC solution should support Active Directory (AD) security best practices, including the identification and remediation of weak passwords, stale accounts, excessive administrative privileges, synchronized administrative accounts, and other risk factors that increase the attack surface.	M	Yes	
34	The proposed NG-SOC solution should provide user mitigation capabilities, such as account locking, disabling, and enforcing multi-factor authentication, to enhance security and minimize potential threats.	D	Yes	
C. Incident Analysis				
1	The proposed NG-SOC service provider solution should support centralized incident management to prioritize and manage security incidents effectively.	M	Yes	
	The proposed NG-SOC service provider solution should support the triaging of alerts from multiple		Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
2	security products, including but not limited to FW, DLP, WAF, XDR, ZTNA, etc.	M		
3	<p>The proposed NG-SOC service provider solution should employ machine-driven triaging algorithms that consider contextual parameters, historical behaviour, and external threat intelligence to enrich alerts and assign a real-time triage score. This triage score will serve as the foundation for prioritizing alerts and determining subsequent actions.</p> <p>Environmental parameters should encompass, but not be limited to, asset criticality, user criticality, and vulnerability status for each alert.</p> <p>Historical parameters should include, but not be limited to, attack volume, attacker volume, destination volume, alert severity, and other relevant factors for each alert.</p> <p>Central Threat Intelligence feeds should be integrated to identify potential threats associated with known bad actors.</p>	M	Yes	
4	The proposed NG-SOC service provider should facilitate the investigation of triaged alerts or custom alerts deemed critical.	M	Yes	
5	The investigation module should seamlessly integrate with log sources (SIEM, XDR, Data Lake) to retrieve data related to the investigated alert on demand. Additionally, it should provide charting and graphing capabilities to analyze the collected data.	M	Yes	
6	The proposed NG-SOC service provider should offer features to assess the impact of an attack on the targeted asset, including configuration changes, Indicators of Compromise (IOCs), and external network connections.	M	Yes	
7	The proposed NG-SOC service provider solution should support features to identify attacker attributes, such as threat intelligence scores, Whois lookup information, and geo- mapping, all within a unified console.	M	Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
8	The proposed NG-SOC service provider solution should employ models to reconstruct the entire attack chain, from its inception and progression to its spread within the network.	M	Yes	
9	The proposed NG-SOC service provider solution should integrate with open-source or commercial IOC sources. Please provide a list of supported sources and a brief overview of the integration approach.	M	Yes	
10	The proposed NG-SOC solution must enable the analysis and identification of the potential impact of an attack on other critical assets by utilizing industry-standard methodologies, such as risk assessment models, asset relationship mapping, or machine learning-based threat correlation. The solution should provide visibility into affected assets and enable prioritization of mitigation efforts based on asset criticality and potential business impact.	D	Yes	
11	The proposed NG-SOC solution must enable the analysis of attack inception and progression through the use of recognized cybersecurity investigation models and frameworks. The solution should support common industry models such as the Cyber Kill Chain, MITRE ATT&CK, or other equivalent methodologies for detecting, analyzing, and correlating attack activities. Vendors must provide details on the investigation models utilized within their solution, including their applicability to the organization's security requirements and the methodology for implementing them.	D	Yes	
12	The proposed NG-SOC service provider solution should enable the analysis and identification of the potential impact of an attack on other assets.	M	Yes	
13	The proposed NG-SOC service provider solution should leverage models to derive attack inception and progression. To enable an NG-SOC solution to derive attack inception and progression, the service provider can utilize various cybersecurity investigation models and frameworks. Please provide details on the investigation models utilized within the solution.	M	Yes	
	The proposed NG-SOC service provider solution		Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
14	should offer case management features to store both raw and analysed data for specific alerts or groups of alerts. Please provide details on the types of artifacts that can be stored in relation to an investigation.	M		
15	The proposed NG-SOC service provider solution should support rapid search capabilities across stored datasets within the solution. Please provide details on the supported search features.	M	Yes	
16	The proposed NG-SOC service provider solution should furnish runbooks outlining investigation steps for various types of attacks.	M	Yes	
D. Incident Response				
1	The proposed NG-SOC service provider solution should support quick response to ongoing incidents or serious threats, enabling remote configuration of parameters in servers, desktops, firewalls, Active Directory, Intrusion Prevention Systems, Web Application Firewalls, network switches, and routers. Automated remediation for responding to commodity threats, such as blocking malicious IP addresses in firewalls, disabling compromised user accounts in Active Directory, and other similar actions, should also be supported.	M	Yes	
2	The proposed NG-SOC service provider solution should support the entire workflow for incident classification, incident coordination (including assigning activities to different teams, tracking closure, escalating tasks, and approving exceptions), and incident resolution.	M	Yes	
3	The proposed NG-SOC service provider solution should support the workflow required to approve automated mitigation actions or provide an option to exempt certain automated mitigations from the approval process.	M	Yes	
4	The proposed NG-SOC service provider solution should support escalation workflows. Detailed information on the escalation matrix, including levels and escalation mediums (SMS or email), should be provided.	M	Yes	
5	The proposed NG-SOC service provider solution should track security exception approvals for threats and incidents where remediation is not feasible or compensating controls are in place.	M	Yes	
6	The proposed NG-SOC service provider solution should integrate with either external service desks or internal ticketing tools to leverage existing service desk platforms.	M	Yes	
	The proposed NG-SOC service provider solution should link and display alert details. The investigation outcomes for relevant remediation		Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
7	tickets is desired.	D		
8	The proposed NG-SOC service provider solution should generate incident reports that include classification, a chronology of events, root cause analysis, and indicators of compromise.	M	Yes	
9	The proposed NG-SOC service provider solution should track assets impacted by an incident.	M	Yes	
10	The proposed NG-SOC service provider solution should have tools for response-based decision-making, leveraging data and analytics.	M	Yes	
11	The proposed NG-SOC service provider solution should enable quick counter- response by integrating with devices such as firewalls and Active Directory to block traffic or quarantine systems.	M	Yes	
12	The proposed NG-SOC service provider solution should utilize ticketing and case management workflows.	M	Yes	
13	The proposed NG-SOC service provider solution should classify incidents.	M	Yes	
14	The proposed NG-SOC service provider solution should track the initial response and subsequent measures taken for each incident.	M	Yes	
15	The proposed NG-SOC service provider solution should maintain a chronological order of events related to incident response.	M	Yes	
16	The proposed NG-SOC service provider solution should maintain indicators of compromise and other artifacts related to incidents.	M	Yes	
17	The proposed NG-SOC service provider solution should conduct endpoint investigations, if necessary, to conclude investigations.	M	Yes	
18	The proposed NG-SOC service provider solution should offer centralized incident management to prioritize and manage security incidents effectively.	M	Yes	
E. Threat Hunting Requirements				
1	The proposed NG-SOC service provider solution should use advanced algorithms and tools to actively hunt for attacks within large volumes of data and generate actionable alerts for analysts. The service should support the utilization of a big data platform for comprehensive data collection and in-depth analysis.	M	Yes	
	The proposed NG-SOC service provider is required to define, develop, implement, update, and maintain		Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
2	a robust Hunting Framework. This framework should include the creation of a knowledge base of Indicators of Compromise (IOCs) to enhance threat detection capabilities.	M		
3	The proposed NG-SOC service provider solution should deliver security analytics as a service, enabling the detection of unknown and sophisticated attacks. The analytics service is expected to employ models capable of identifying threats at various stages of the cyber kill chain.	M	Yes	
4	The proposed NG-SOC service provider solution should ensure that the analytics service can detect threats arising from diverse attack vectors, such as malware, web application attacks, network attacks, watering hole attacks, DNS attacks, insider threats, and data exfiltration. The service should list detection use cases that leverage prebuilt machine learning techniques and analytical models for identifying these types of attacks.	M	Yes	
5	The proposed NG-SOC solution should leverage machine learning techniques to analyze data from multiple and varied sources to detect malicious activities. These sources may include, but are not limited to, NetFlow, Web Application Firewall (WAF) logs, Windows event logs, DNS traffic, Firewalls, and any other relevant data sources that contribute to comprehensive threat detection. The solution should support flexibility to incorporate new and evolving data sources over time.	D	Yes	
6	The proposed NG-SOC service provider solution should ensure that the solution includes prebuilt AI models designed to detect targeted attacks, including unknown threats originating from previously unidentified threat actors. Additionally, analytical models should be implemented to identify activities across different stages of the Cyber Kill Chain.	M	Yes	
7	The proposed NG-SOC service provider should solution perform network threat hunting by leveraging existing network sources to enhance the detection of advanced threats. These network sources should include, but are not limited to, NetFlow, Proxy, DNS, IPS, VPN, Firewall, AD/Windows logs, and Email logs.	M	Yes	
	The proposed NG-SOC service provider solution should incorporate AI capabilities in network threat hunting to detect various attack types, including		Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
8	lateral movement, malware beaconing, data exfiltration, watering hole attacks, targeted network intrusions, and dynamic DNS attacks.	M		
9	The proposed NG-SOC solution must have the capability to identify suspicious or previously undiscovered communication patterns using established detection techniques such as anomaly detection, behavioral analytics, or machine learning. The solution should be adaptable to detect newly emerging patterns through flexible, scalable approaches that can evolve as threats and attack methods change over time. Vendors should provide details on the methods, models, and technologies used to detect communication patterns, ensuring future-proof capabilities while remaining aligned with current industry standards.	D	Yes	
10	The proposed NG-SOC service provider solution should include features to identify network traffic originating from potentially risky applications, such as file-sharing and peer-to-peer platforms, ensuring enhanced security visibility and control.	M	Yes	
11	The proposed NG-SOC service provider should have dedicated inhouse threat research and threat hunting team.	M	Yes	
F. Threat Intelligence				
1	The proposed NG-SOC solution should have the capability to analyze global and regional threat intelligence data to identify potential threats to the organization. The solution should provide actionable insights to mitigate these threats, ensuring that organizations can take appropriate measures to prevent incidents. Vendors are encouraged to provide details on the threat intelligence sources utilized and the methodologies for deriving actionable measures, ensuring a flexible and adaptive approach to threat detection and prevention.	M	Yes	
2	The proposed NG-SOC service provider solution should provide strategic threat intelligence on global incidents and breaches, offering actionable insights such as: Assessing whether NFSU could be vulnerable to a specific attack. Identifying which organizational assets may be at risk. Delivering relevant Indicators of Compromise (IoCs). Suggesting detailed mitigation steps for each	M	Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
	advisory.			
3	The proposed NG-SOC solution should leverage threat intelligence to analyze organizational assets, network traffic, security events, and user activities, generating reports on potential risks and their impact on each entity. The solution should provide recommendations for risk mitigation measures, which may include both proactive and reactive actions, depending on the identified threats. Vendors should specify the methodologies used to analyze threat intelligence and how recommendations are provided, ensuring flexibility in threat response.	M	Yes	
4	The proposed NG-SOC service provider solution should track the status of assets against IoCs and CVEs while enabling a workflow to manage remediation efforts. For example, vulnerabilities from shadow broker releases should be used to identify affected assets, and the workflow must ensure CVEs are addressed and tracked to closure through patching or other mitigation activities. The service provider should monitor closure statuses and quantify risk reduction.	M	Yes	
5	The proposed NG-SOC service provider solution should include capabilities to automatically assess and assign business value to organizational assets, ensuring critical resources are prioritized effectively. Machine learning algorithms or equivalent automated techniques may be used to achieve this objective.	M	Yes	
6	The proposed NG-SOC service provider solution should ensure compatibility with STIX/TAXII standards to enable automated integration of actionable intelligence with existing security technologies.	M	Yes	
7	The proposed NG-SOC service provider solution should support the incorporation of third-party or external threat intelligence to enhance incident response capabilities. This should include leveraging organizational context and internal data from sources such as SIEM and other security tools.	M	Yes	
8	The proposed NG-SOC service provider solution should deliver comprehensive vulnerability management reports detailing the organization's vulnerability status and providing actionable mitigation recommendations.	M		
	The proposed NG-SOC service provider should integrate vulnerability information with the threat management system to offer a holistic, 360-degree		Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
9	view of each asset, ensuring complete situational awareness.	M		
10	The proposed NG-SOC service provider should be able to monitor the cyber risk index of an organization and alert regarding risk assessment of Users, Devices and Applications Above information can be used to leveraged for faster detection and response using corelation and analytics.	M	Yes	
11	There are many Global active campaigns going in the wild so the NG-SOC service providers supposed to do Proactive sweeping of IOC's of global Attack campaigns in the data lake and alert, if found.	M	Yes	
12	The proposed NG-SOC service provider should have option that NFSU / NFSU's Client may want to do Manual Sweeping of IOC's received from the different sources, it will be uploaded to the Platform or shared with the service team for the further actions.	M	Yes	
13	The proposed NG-SOC service provider should have an option of uploading suspicious files by customers team or submit to the analyst.	M	Yes	
14	The proposed NG-SOC service provider should share of IOC's generated as part of investigation and response should be mandatorily shared with other Security tools i.e. Firewall, Proxy	M	Yes	
G. Endpoint Desktop and Server Detection & Response Service				
1	The proposed NG-SOC service provider solution should collect telemetry/activity data from all relevant sources configured within the present XDR solution of NFSU / NFSU's Client, including endpoints, servers.	M	Yes	
2	The proposed NG-SOC service provider solution should facilitate real-time log collection and ingestion to ensure minimal latency in detecting and responding to security incidents.	M	Yes	
3	The service provider should solution comply with NFSU / NFSU's Client regulatory and business requirements for log retention and storage, ensuring scalability for long-term storage and quick retrieval during investigations.	M	Yes	
4	The proposed NG-SOC service provider solution should correlate logs across multiple sources ingested into the XDR solution to detect multi-vector and advanced persistent threats (APTs).	M	Yes	
5	The proposed NG-SOC service provider solution should utilize contextual data, such as threat intelligence feeds, asset criticality, and geolocation, to enrich logs and provide meaningful insights during correlation.	M	Yes	
	The proposed NG-SOC solution should have the		Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
6	capability to identify anomalous behavior patterns by correlating logs with baseline behavior profiles for users and devices. The solution should be flexible enough to integrate with existing end point security isolation , i.e. NFSU / NFSU's Client present XDR solution, while allowing for compatibility with third-party tools that can provide similar detection capabilities.	M		
7	The proposed NG-SOC service provider solution should ensure that the correlation engine identifies both signature-based threats (using IoCs) and emerging threats (using machine learning and heuristic analysis).	M	Yes	
H. User and Entity Behavior Analytics (UEBA)				
1	The proposed NG-SOC service provider solution should have the capability to identify and detect any malicious or unauthorized activities conducted by users within the network.	M	Yes	
2	The proposed NG-SOC service provider solution is expected to collect and process user-related data from various sources, including Directory Services, Identity and Access Management (IAM) systems, VPNs, Proxy servers, O365 platforms, and others.	M	Yes	
3	The proposed NG-SOC service provider solution should incorporate baseline behavioral models to detect and address a wide range of security risks, including malicious user actions, illicit behaviors, and the use of compromised credentials. The solution should be flexible enough to support different methods of data collection and analysis, including endpoint telemetry, network traffic analysis, and other relevant data sources, while allowing for agent-based or agentless deployment as appropriate.	M	Yes	
4	The proposed NG-SOC solution is required to support business application threat hunting by leveraging application logs to identify anomalies in access and authorization.	M	Yes	
5	The proposed NG-SOC service provider solution should be capable of proactively searching through network and log data to detect and isolate advanced threats that evade traditional signature-based systems such as SIEM, IDS, and DLP.	M	Yes	
6	The proposed NG-SOC service provider solution should enable the advanced detection of targeted web application attacks by analyzing security events from Web Application Firewalls (WAF) and other relevant sources. This capability may incorporate	D	Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
	machine learning, AI models, or other automated techniques to enhance detection accuracy and response effectiveness.			
7	The proposed NG-SOC service provider should be capable to continuous discovery of the risks of known, unknown, internal, and external assets.	M	Yes	
8	The proposed NG-SOC service provider should have a process to tag Asset criticality which indicates the importance of an asset to organization's operations.	M	Yes	
9	The proposed NG-SOC service provider should continuously scan and assess your assets for known vulnerabilities and misconfigurations that could be exploited by attackers.	M	Yes	
10	The proposed NG-SOC service provider should identify at-risk users and devices and provides remediation and suggested preventative options to manage the risk to organization environment.	M	Yes	
11	The proposed NG-SOC service provider should assign risk scores to assets and vulnerabilities based on severity and potential impact, helping prioritize remediation efforts.	M	Yes	
12	The proposed NG-SOC service provider should have a view detailed information about a selected device, internet-facing asset, user account, cloud app or cloud asset.	M	Yes	
13	The proposed NG-SOC service provider should provide rich context for threat investigation and hunting using a graphic visualization of the relationships between all assets in the Asset Graph.	M	Yes	
14	The proposed NG-SOC service provider should automatically calculate Asset Criticality using asset attributes, activities, and interactions with other assets.	M	Yes	
15	The proposed NG-SOC service provider should prioritize risks and implement targeted Risk Reduction Measures aligned with organization's goals.	M	Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
16	The proposed NG-SOC service provider should review the top risks associated with Cloud App activity in organization.	M	Yes	
17	The proposed NG-SOC service provider should select a risk reduction goal and remediate risk events with the highest impact on the risk index.	M	Yes	
I. SECURITY ORCHESTRATION AUTOMATION AND RESPONSE (SOAR)				
1	The proposed NG-SOC service must include SOAR capabilities to enable security orchestration, automation, and response. These capabilities may be provided through a standalone SOAR platform or as part of an integrated solution, ensuring seamless automation of workflows and incident management.	M	Yes	
2	The solution should support a wide range of integrations with third-party tools, including but not limited to forensic tools, IT systems (e.g., AD, SAML), communication tools (e.g., email, Slack, Hipchat), SIEM, endpoint security, network security, threat intelligence, and others. The solution should provide integration packs with pre-built use cases, playbooks, automation actions, and scripts, while also enabling customization of these features. Additionally, the solution should offer regularly updated with both vendor and partner-provided integrations.	D	Yes	
3	The proposed NG-SOC service provider should offer pre-configured playbooks aligned with standards such as SANS and NIST for incidents like malware, phishing, and DoS, while supporting the creation of custom playbooks based on SOC-specific use cases.	M	Yes	
4	The proposed NG-SOC service provider should enable incident response playbooks that consist of defined phases and tasks to guide users in responding effectively to incidents, integrating people, processes, and technology seamlessly.	M	Yes	
5	The proposed NG-SOC service provider should allow organizations to simulate incidents to test response plans, enabling them to identify gaps and refine processes proactively before real incidents occur.	M	Yes	
	The proposed NG-SOC service provider should include out-of-the-box capabilities to query or add		Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
6	IOCs/artifacts to the existing reference set of the deployed SIEM solution.	M		
7	The proposed NG-SOC service provider should offer access to resources such as community portals, knowledge bases, training materials, or forums where users can learn about sample integrations, resolve issues, and discuss use cases or best practices. These resources should facilitate ongoing education and collaboration to enhance the user experience and address specific needs.	M	Yes	
8	The proposed NG-SOC service provider should integrate seamlessly with incident management tools and third-party IT ticketing systems.	M	Yes	
9	The proposed NG-SOC service provider should ensure compatibility with the organization's existing investments in security platforms, including XDR, while offering an architecture that avoids vendor lock-in.	M	Yes	
10	The proposed NG-SOC service provider should provide a hybrid/multi-cloud architecture to accommodate diverse deployment needs.	M	Yes	
11	The proposed NG-SOC service provider should deliver a single, integrated platform capable of analyzing logs, flows, vulnerabilities, user data, and asset data to offer comprehensive visibility into networks, applications, and user activities.	M	Yes	
12	The proposed NG-SOC service provider should automatically map investigation outputs to MITRE ATT&CK tactics and techniques to streamline incident analysis.	M	Yes	
13	The proposed NG-SOC service provider should include a visual editor or canvas for creating playbooks/runbooks, allowing users/security analyst to design workflows without coding through native integration with third-party tools and processes.	M	Yes	
	The proposed NG-SOC service provider should offer a comprehensive set of built-in, reusable playbooks for common incident types such as phishing,		Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
14	malware, and IOC hunts, as well as the flexibility to create and customize playbooks for additional incident types.	M		
15	The solution should provide flexible, customizable playbooks that can be tailored to cover critical use cases such as incident response, threat hunting, and threat intelligence integration. These playbooks should support, but not be limited to, the following areas: Phishing incident response Malware infection response Threat hunting using indicators of compromise (IOCs) across security logs and devices Mapping to frameworks such as MITRE ATT&CK with appropriate actions Integrating threat intelligence scoring and actionable deployment to security devices.	D	Yes	
16	The proposed NG-SOC service provider should support the creation of custom playbooks to map out specific CIRT processes, with the flexibility to build and customize playbooks within the solution.	M	Yes	
17	The proposed NG-SOC service provider should support the reuse of existing playbooks as components of larger, more complex playbooks.	M	Yes	
18	The proposed NG-SOC service provider should allow playbooks to include a mix of manual, automated, and conditional tasks.	M	Yes	
19	The proposed NG-SOC service provider should ensure that a single playbook can effectively combine automated and manual tasks within the same workflow, enabling both human intervention and automation as needed.	M	Yes	
20	The proposed NG-SOC service provider should provide the capability to execute entire playbooks either automatically or manually, while clearly listing any exceptions.	M	Yes	
21	The proposed NG-SOC service provider should support step-by-step debugging for running playbooks, with provisions to resume execution from the point of failure.	M	Yes	
22	The proposed NG-SOC service provider should allow for the addition of ad hoc tasks within an existing playbook.	M	Yes	
23	The proposed NG-SOC service provider should support the scheduling of playbooks to run at predefined intervals.	M	Yes	
	The proposed NG-SOC service provider should include functionality for passing parameters between		Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
24	upstream and downstream tasks within a playbook.	M		
25	The proposed NG-SOC service provider should support updates for playbooks and integrations, while clearly defining the procedures for updating these components.	M	Yes	
26	The proposed NG-SOC service provider should have an option of embedding multiple Playbooks and create a playbook chaining.	M	Yes	
27	The proposed NG-SOC service should be multiple types of playbooks by default i.e. Fetch, Response, Threat and Incident playbooks as part of service.	M	Yes	
28	The proposed NG-SOC service Curated Playbook needs to be created as per the Security tools deployed in customer's premise. Building connector and creation playbook no additional cost.	M	Yes	
29	The proposed NG-SOC service provider should be able to Ticket creation and auto assignment for alerts	M	Yes	
30	The proposed NG-SOC service provider should Enrichment with critical contextual data helps both the system and analysts more quickly and accurately understand the security context and impact of a detection. Context and Sources IP Address Hash Email Sender Url User Geo location	M	Yes	
31	The proposed NG-SOC service provider should have multiple sources for enrichment like example Virus Total, Phish Tank, Abuse IP, CheckFish etc.	M	Yes	
j. Response and Remediation as part of NG-SOC				
1	The proposed NG-SOC service provider should able to take confident response actions on their own with limited dependencies on NFSU / NFSU's Client	M	Yes	
2	The proposed NG-SOC service provider should provide the capability to tag assets for automated response. NFSU / NFSU's Client will assist in categorizing the assets into Critical and Non- critical assets. The solution should support asset tagging either natively or via integration with existing asset management systems.	M	Yes	
3	The proposed NG-SOC service provider should be able to guide the remediation action for the team.	M	Yes	

Next Generation Security Operation Centre Service				
S. No.	Capabilities/Description	Priority	Compliance (Yes/No)	Remarks
4	The proposed NG-SOC service provider should have Supported response actions - isolation, kill, terminate, remote shell, process memory dump, email quarantine, block file hash/IP/URL, collect file and running tool kit.	M	Yes	
5	The proposed NG-SOC service should be able to integrate with the tools deployed across NFSU's Client, AD on-prem, Azure AD, VA scan tools, Ticketing supporting various use case with no additional cost.	M	Yes	
6	NFSU/NFSU's Client's Security Team should have access to the analyst	M	Yes	
7	NFSU/NFSU's Client's needs Email, Phone, and Messaging mode to reach out to SOC team	M	Yes	
8	The proposed NG-SOC service provider should provide Escalation matrix for reporting suspicious activities.	M	Yes	
K. Dashboards and Reporting				
1	NFSU / NFSU's Client team should be able to see number of cases / incidents generated and status	M	Yes	
2	NFSU / NFSU's Client team should be able to see number of alerts generated and status	M	Yes	
3	The proposed NG-SOC service provider dashboard should be able to show the Resolution time status of the tickets.	M	Yes	
4	NFSU / NFSU's Client should get Executive Reports and Technical reports	M	Yes	
5	Using Dashboards - Service should be able help customers track SLO's.	M	Yes	
6	The proposed NG-SOC service provider should have dashboards to measure MTTD and MTTR	M	Yes	
7	The NFSU / NFSU's Client SOC dashboard should include threat intelligence, SOC data such as product-wise log and alert details, and incident response information. The customer should be able to view the status and have search capabilities to query logs.	M	Yes	

Note:

a) “M” stands for Mandatory specification, “D” stands for Desired specification.

**ANNEXURE - 1 Undertaking with respect to Compliance of
Restrictions for Countries which share land border with India - as
stipulated by Govt. of India.**

(On Company Letter Head, to be signed by the duly authorized person)

Date:

BID NO.:

TITLE

OF

BID:

.....

To,

**The Campus Director,
National Forensic Sciences University
Sector - 9, Gandhinagar, Gujarat - 382007**

Dear Sir,

In line with the guidelines issued for compliance of Restrictions for Countries which share land border with India - as issued by Govt. of India in July'2020,

I/We have read the clause regarding restrictions on procurements from a bidder of a country which shares a land border with India and on sub-contracting to contractors from such countries.

- I/We certify that _____ is not from such a country or if from such a country has been registered with the competent authority. I/We hereby certify that _____ fulfils all requirements in this regard and is eligible to be considered*.
- I/We certify that _____ is not from such a country or if from such a country has been registered with the competent authority and will not sub-contract any work to a contractor from such countries unless such contractor is registered with the competent authority. I/We hereby certify that _____ fulfils all requirements in this regard and is eligible to be considered*. (Applicable for works involving possibility of sub-contracting)
- I/We have read the clause regarding restrictions on procurement from a bidder having Transfer of Technology (ToT) arrangement. I/We certify that _____ does not have any ToT arrangement requiring registration with the competent authority.
- I/We hereby certify that I/We fulfill all requirements in this regard and am/are eligible to be considered.

[* Where applicable, evidence of a valid registration by the Competent Authority shall be attached]

(Signature of the Authorized Signatory)

Name:

Seal:

ANNEXURE - 2: NO BLACKLIST DECLARATION

(To be submitted on the Bidder's letterhead)

Ref. No:

To

Campus Director
National Forensic Sciences University
Sector - 9, Gandhinagar, Gujarat - 382007.

Sub: No Blacklisting Self-Declaration for Tender Ref. No: for "Notice inviting bid for Selection of Managed Next-generation SOC (NG-SOC) Service Provider"

Dear Sir/Madam,

We do hereby declare and affirm that we have not been blacklisted/debarred by any Government departments, Agencies or Public Sector Undertakings in India in last 5 years as on the date of submission.

(Authorized Signatory of Bidder)

Date: (Company Seal)

ANNEXURE - 3 MALICIOUS CODE CERTIFICATE
(To be submitted on the Bidder's letterhead)

Ref No.

Date.

To,
The Campus Director,
National Forensic Sciences University
Sector - 9, Gandhinagar, Gujarat - 382007

Sub: Malicious Code Certificate

This is to certify that the Hardware and the Software being offered as a part of NG-SOC service, does not contain Embedded Malicious code that would activate procedures to:

Inhibit the desires and designed function of the equipment.

Cause physical damage to the user or equipment during the exploitation.

Tap information resident or transient in the equipment/network.

This is also certify that our firm will be considered to be in breach of the procurement contract, in case physical damage, loss of information or infringements related to copyright and Intellectual Property Right (IPRs) are caused due to activation of any such malicious code in embedded software.

(Authorized Signatory of Bidder)

Date: (Company Seal)

**ANNEXURE - 4 Acceptance Of Terms & Conditions of Tender
Undertaking**

(Duly sealed and signed certificate on Company/Firm's Letterhead)

To,
The Campus Director,
National Forensic Sciences University, Gandhinagar
Subject: Acceptance of Terms & conditions of Tender.
Tender ref: tender No. dated

Dear Sir,

I/We have Downloaded/obtained the tender document(s) for the above-mentioned Tender enquiry no. from the CPPP portal/website.

I/We hereby certify that I/we have read entire terms & conditions of the tender documents (including all documents like annexure, schedules etc.) along with Additional terms and conditions (ATC) which form part of the tender document and I/we shall be abiding by the terms & conditions/clauses contained therein

The corrigendum(s) issued from time to time by NFSU, Gandhinagar Campus to have also been taken into consideration, while submitting this acceptance letter.

I/We do hereby declare that I/We have read and understood the entire specifications/requirements laid down in the tender document and have prepared the bid compliance with the requirements specified in the document.

I/We hereby unconditionally accept the tender conditions of above-mentioned tender document(s)/corrigendum(s) in totality/entirely.

In case any provisions of this tender are found violated, NFSU, Gandhinagar Campus shall bear liberty to reject this tender/bid and we shall not have any claim/right against NFSU, Gandhinagar Campus in satisfaction of this condition.

Date:

(Seal & Signature of the bidder)

ANNEXURE - 5 -EMD/Bid Security Form

**To,
The Campus Director,
National Forensic Sciences University, Gandhinagar**

**Subject: Format of Bid Security Declaration from bidders in lieu of
Earnest Money Deposit / Bid Security (On Bidders' Letter Head)**

Tender ref: _____ dated _____

I /We, the authorized signatory of M/s_____ ,participating in the Tender No: _____, do hereby declare that in the event of:

1. Withdrawing / Modifying our bid during the period of bid validity
OR
2. Committing any other breach of tender conditions/ contract which would have attracted forfeiture of EMD OR
3. Failure/ refusal to initiate the execution of the awarded Contract as per the terms of the Contract

I / We could be suspended from being eligible for bidding / award of all future tender(s) for a period as per the GFR and relevant Govt Orders.

Date:

(Seal & Signature of the bidder)