General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
	Cyber Risk Protector Insurance Proposal Form		
1	**Company Information**	Name of Proposer	GENERAL INSURANCE CORPORATION OF INDIA
		Web site	www.gicre.in
		Principal address of Proposer	"SURAKSHA", 170 J TATA ROAD, CHURCHGATE, MUMBAI – 400020, INDIA.
		Business Description	ReInsurance
		Geographical Exposure	Total Gross Revenue (Gross Premium Written): Rs 41,955.33 Crore (FY 2024-25) Rs 44,367.88 Crore (FY 2025-26) Geographical Split of the Company's Total Gross Revenue (%) a. European Union: Rs. 1,650.08 Crore (FY 2024-25) Rs. 1,098.94 Crore (FY 2025-26) b. United States: Rs. 224.59 Crore (FY 2024-25) Rs. 195.57 Crore (FY 2025-26) Rest of World: Rs. 40,080.66 Crore (FY 2024-25) Rs. 43,073.37Crore (FY 2025-26)
		Desired Coverage	✓Cyber/Privacy Extortion ✓MultiMedia Liability ✓Network Interruption
		(a)Is there a written data protection policy and privacy policy that applies to the Company?	Yes ; The Corporation has implemented all applicable regulatory and technical controls to protect the confidentiality and integrity of data. Multiple control policies are maintained as part of the Corporation's Information Security Policy and Procedures.
		b) Are all employees provided with a copy and any update of the Company's data protection policy which they are required to confirm compliance with?	Yes

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
2	**Data Protection Procedures**	c) When was the Company's data protection policy last reviewed and by whom?	In FY 2025-26 External CERT-In Empanelled IS Auditor has reviewed Information Security Policy and Procedures.
		d) Does the Company's data protection policy comply with the data protection and privacy legislation applicable to all jurisdiction and Industry standards/requirements, in which the Company operates?	Yes
		e) Have the Company's U.S. Subsidiary(ies) signed-up for, and are they compliant with, the Safe Harbor Program between the United States of America and the European Union?	NA
		f) Does the Company employ a Chief Compliance Officer, Data Protection Officer and/or In-house Counsel responsible for data protection related matters?	Yes ; CISO
3	**Data Access & Recovery**	a) Does the Company use firewalls to prevent unauthorized access connections from external networks and computer systems to internal networks? If "Yes" are all computer systems, mobile devices and websites Firewalled or have intrusion prevention systems on them?	Yes
		b) Does the Company use anti-virus protections and procedures on all desktops, e-mail systems and mission critical servers to protect against viruses, worms, spyware and other malware? If "Yes," how often are such protections and procedures updated?	Yes ; Daily
		c) Does the Company have in place procedures to identify and detect network security weaknesses?	Yes
		d) Does the Company monitor its network and computer systems for Breaches of Data Security?	Yes
		e) Does the company have physical security controls in place to prohibit and detect unauthorized access to their computer system and data centre?	Yes
		f) Does the Company collect, store, maintain or distribute credit card or other sensitive personally identifiable data? (i)If "Credit Card" is selected above, does the company comply with Payment Card Industry Data Security Standards? (ii)If either is selected, is the access to such sensitive data restricted? (iii)Who has access?	Personally identifiable data; (i) No; (ii)Yes; (iii)The Corporation maintains employees PII with access restricted to HR department.
		g) Does the Company process payments on behalf of others, including eCommerce transactions?	No

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
		h) Does the Company have encryption requirements for data-in-transit data-at-rest to protect the integrity of Sensitive Data including data on portable media (e.g., laptops, DVD backup tapes, disk drives, USB devices, etc.)? If "Yes", please describe where such encryption is used:	Yes, all laptops and desktops used by the organization are encrypted using bitlocker. DVDs, USBs, etc. are not allowed.
		i) Does the Company have and maintain backup and recovery procedures for all: i) mission critical systems? ii) data and information assets? If "Yes" is it encrypted?	Yes (i) Yes (ii) Yes, Encrypted.
		j) Does the Company perform background checks on all employees and independent consultants?	Yes
		k) Does the Company require remote users to be authenticated before being allowed to connect to internal networks and computer systems?	Yes
4	**Outsourcing Activities**	a) Does the Company outsource any part of its network, computer system or information security functions? If "Yes" who is the security outsourced to? And does the Applicant periodically audit the functions of the outsourcer to insure that they follow the Applicant's security policies?	Yes ; MEITy empaneled DC service provider
		b) Does the Company outsource any data collection and/or data processing?	No
		c) Does the Company require the entities providing data collection or data processing functions (Outsourcers) to maintain their own data protection liability insurance?	No
		d) Does the Company require indemnification from Outsourcers for any liability attributable to them?	Yes
		e) How does the Company select and manage Outsourcers?	Bidding through GeM
		f) Does the Company require all Outsourcers to comply with the terms of the Company's data protection policy?	Yes
5	**Claims Information**	a) Has the Company been the subject of any investigation or audit in relation to data protection by a Data Protection Authority or other regulator?	No
		b) Has the Company ever been subject to a Data Subject Access Request?	No
		c) Has the Company ever been subject to an Enforcement Notice by a Data Protection Authority or any other regulator?	No

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
		d) Is the Company after due inquiry aware of any actual or alleged fact or circumstance which may give rise to a claim under this policy?	No
6	**Additional Details**	Nationality	Indian
		Type of Organization	Corporation; Government
		PAN card number (10 character number)	AAACG0615N
		Sources of funds	Business

Commercial Crime Proposal form

1	**Proposer Details**	Name of Proposer	GENERAL INSURANCE CORPORATION OF INDIA
		Principal address of Proposer	"SURAKSHA". 170 J TATA ROAD, CHURCHGATE, MUMBAI – 400020, INDIA.
		Date established	22nd November, 1972
		Principal activities/services of Proposer	Reinsurance
		Number of permanent directors	Not applicable
		Number of employees: (a)Domestic : (b)Overseas :	(a) 498 (b) 26
		Number of locations: (a)Domestic (b)Overseas	Domestic: Head Office, One branch office in Gift City & 1 Liaison Offices (Delhi); Overseas: 3 Branches (London, Dubai and Malaysia), 3 Subsidiaries (GIC Re South Africa Ltd., Johannesburg; GIC Re, India, Corporate Member Limited, London and GIC Perestrakhovanie LLC, Moscow) and 1 Joint Venture (GIC Bhutan Re Ltd., Bhutan).
		Current Market Value of all Pension and Employee Benefit Plans	Rs 487.50 Crore
		(i)Please list all acquisitions and mergers you have made in the past 5 years and indicate the turnover for each acquisition: (ii)Are all recommendations arising from the pre-acquisition due diligence process immediately implemented? If "no", please provide details	Not Applicable
		Does the company have an employee Handbook/Manual? If "yes" (a) does it contain written instructions on all aspects of your business? (b) does it clearly define the individual duties of each employee? (c) does it address security procedures (including electronic data security)?	Yes (a)Yes (b)Yes (c)Yes

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
2	**Internal Controls and Procedures**	Are employees trained and re-trained, if necessary, on all aspects of: (a)physical and electronic data security? (b)operational procedures?	(a)Yes (b)Yes
		Are all employees required to take an uninterrupted, two week holiday each calendar year?	No
		Are the duties of each employee arranged so that no one employee is permitted to control any transaction from commencement to completion?	Yes
		(a)Please provide details of the groups recruitment policy including details of your assessement of the suitability for all positions (b)Please describe your employee leaving procedures. (c)Please describe your staff rotation procedures.	Employees are categorized into sensitive and non sensitive posts and job rotation policies are followed
		Are any branches, subsidiaries or associated companies allowed to maintain different operational procedures than the Head Office/Parent Company? If “yes”, is prior approval required from Head Office/Parent Company?	Branches: No; Subsidiaries or Associated Companies: Yes; No
		Do you maintain dual control over the handling of: (a)securities? (b)company/corporate cheques and drafts? (c)dormant accounts (if dormant for longer than 6 months)? (d)access codes, cyphers, test keys?	Yes
		Is joint custody maintained for the safeguarding of: (a)access codes, cyphers, test keys? (b)access to Property whilst in safes and/or vaults?	Yes
		Do you operate or subscribe to any automated teller machine network or electronic point of sale system?	No

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
3	**Computer Systems**	Do you make or receive funds transfer instruction via any of the following methods and what are the average daily transfer limits against each method used?: (a) Interbank electronic communications systems (i) BACS (ii) SWIFT (iii) CHAPS (iv) Bankwire (v) Other, please specify (b) Internet (c) Electronic mail (d) Telex (e) Facsimile (f) Voice initiated (g) On-line cash management (h) Other, please specify	(a) Yes (b) Yes (c) No (d) No (e) No (f) No (g) No (h) NA
		Are all fund transfer instructions subject to a verification and authentication process?	Yes
		Do you secure fund transfer instructions (e.g. through the use of passwords, encryption, testing, call back or other authentication)?	Yes
		Do you permit the transfer of funds via telephonic instruction?	No
		Are passwords used to give varying levels of access to your computer system and funds transfer systems on the need and authorisation of user basis?	Yes
		Are all key source documents maintained in a secure environment prior to being entered into the computer system in order to prevent unauthorised modification or inappropriate use of data?	Yes
		Are remote terminals kept in a physically secure location accessible by authorised personnel only?	Yes
		Do you utilise any recognised software packages to control access to your computer system?	No
		Are your data processing centers physically separated from other departments?	Yes
		Do you have an access control system for your data processing centers?	Yes

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
		Are data file generations stored and secured off-site in a restricted area?	Yes
		Do you utilise independent contractors to prepare electronic computer programs? If "yes": (a)are specific parameters in place to restrict their access? (b)are their activities overseen when accessing your computer system? (c)are safeguards in place to prevent access to your other systems?	Yes; (a) Yes (b) Not applicable (c) Yes
4	**Internet Facility/ E-Commerce**	Do you provide an Internet facility?	No; Internet facility is available for Corporation's employees.
		Do you have formal terms and conditions for the use of your Internet facility, which outline the obligations and responsibilities of the users?	Yes
		Is the identity of users verified and authenticated?	Yes
		Do you encrypt data whilst it is stored or held within your Internet facility?	Yes
		Are firewalls and/or comparable software used to authorise access to your Internet facility?	Yes
		Do you use any anti-virus software? If "yes" is this upgraded on a regular basis?	Yes
		Do you monitor and produce reports on intrusion/ unauthorised access activity?	Yes
		Do you restrict access between your Internet facility and your main computer system?	Yes
		Do you have a specific department which maintains your Internet facility (e.g. carrying out program development,testing, firewall maintenance, intrusion monitoring)?	Yes
		When was your last independent Ethical Hacking Test, by who was it carried out and what vulnerabilities were highlighted? What remedial action did you take?	For vulnerability identification, detection & remediation, VAPT done for every quarter & Annaul IS audit done as per applicable IRDAI Guidelines by CERT-In empaneled auditor firm. Network, system and applications, websites, domain & physical related securities are checked and complied.; As per audit recommendation, actions are taken.
		Do you have a fully tested disaster recovery and business continuity plan? If "yes", does it include an off-site back-up facility?	Yes

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
5	**Lending Procedures**	Do you operate and maintain a formal loan policy manual or similar internal document?	NA
		Are all loans independently reviewed to ensure compliance with the loan policy manual or similar internal document?	NA
6	**Fund/Investment/Asset Management Companies**	Only complete if the Proposer offers such services to third parties	NA
7	**Insurance Companies (Only complete if the Proposer offers such services to third parties)**	Do you operate and maintain a formal underwriting manual in respect of all classes of insurance written?	Yes
		Please indicate where business production is obtained from as a percentage of the following: (a)agents on commission (b)direct sales (c)brokers/consultants (d)other, please specify	Being a reisurance Company Corporation doesn't engage agents/consultants and significant portion of domestic business is generated on direct basis.
		Are clients/brokers/agents instructed to pay premium in the Proposer's name?	No Applicable, being a reisurance Company.
		Is the department/ individual designated to receive premium completely divorced from the day to day handling of business?	No Applicable, being a reisurance Company.
		Is responsibility for claims inspection/settlement completely divorced from underwriting?	Yes
		Are all claims examined and agreed by a minimum of two authorised individuals before payment is made who ensure that claim payments are made direct to your insured?	Yes

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
8	**Audit and Compliance**	Do you have an internal audit department which has separate duties from the auditing services provided by an external accountant? If "yes", (a)is there a formal written audit programme which includes EDP audit? (b)is there an established audit cycle which encompasses all operations? (c)are the internal audit department independent of any other function? (d)are written reports made to either an audit committee or an individual that reports to the Board of Directors? (e)do you have procedures in place to monitor the implementation of recommendations made by the internal audit department? (f)does the audit team periodically review the segregation of duties, accuracy of records, management and supervisory procedures and the physical and non-physical internal controls?	Yes; (a) Yes (b) Yes (c) Yes (d) Yes Audit Committee (e) Yes (f) Yes
		(a)are you audited annually by a chartered accountant? (b)do they review the internal controls and report their findings? (c)has your accountant made any recommendation in the last two years? If "yes", (i)have such recommendations been complied with? If "no", (ii)have you adopted alternatives arrangements to the satisfaction of your accountant?	(a) Yes; (b) Yes; (c) Audit recommendations are complied within agreed timelines.
		Do you have a compliance officer who monitors and implements all regulatory directives, rules, principles and guidelines?	Yes
9	**Values at Risk**	Please state the maximum value of securities (including negotiable collateral, unissued stock certificates etc.): (a)at head office (b)at branches (c)with custodians	Investment in Securities of the Corporation is managed by the Investment department of the Corporation at HO. Investment by overseas branches are limited to short term deposits with Banks registered with regulatory authorities.
		Please state the maximum amount of cash: (a)at head office (b)at branches (c)at individual tellers (d)within automated teller machines (e)with custodians	(a) NIL (b) Less than INR 50,000/- (c) Not Applicable (d) Not Applicable (e) Not Applicable

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
		Please state the maximum amounts/ values carried by: (a)armoured motor vehicle: (i)cash (ii)securities (b)messengers: (i)cash (ii)securities	Not applicable
10	**Loss Information**	Please give brief details of any loss sustained by the Proposer (whether insured or uninsured) during the past 5 years as follows: (a) Nature of Loss (b) Date of Discovery (c) Location (d) Amount of Loss	(a) Mail Spoofing incident (b) 13th April 2022 (c) GIC Head Office (d) USD 326,500.70
		Does the Proposer, after full enquiry, or any of its directors, officers, partners or trustees have any knowledge, of any act, omission, fact, event or circumstance which might give rise to a loss under this proposed insurance?	No
		In the event that a loss has been discovered, has the Proposer taken remedial action to prevent or avoid recurrence?	Corrective measures taken include updating SOP of Accounts Operation with specific clause “Addition/Change of new/existing Banking details”
11	**Audit and Corporate Governance**	Do External Auditors audit all operations at least annually?	Yes
		(a)Have all recommendations by External Auditors regarding internal controls been complied with following your last audit? (b)If “no”, please provide details	Yes; All critical recommendations are being implemented on priority and other recommendations are implemented as per agreed schedule.
		Is there an Audit Committee which monitors the effectiveness of internal controls and reports directly to the Board?	Yes
		a)Do you comply with all provisions of the Combined Code of Corporate Governance relating to Financial Aspects of your business? (b)If “no”, please briefly explain reasons for areas of non-compliance	Yes
		(a)Do you have an Internal Audit Department? (b)Do they have an established audit cycle for all operations?	Yes
		(a)Do you have a Treasury Department? (b)Do they have a procedures manual specifying authority levels for each member of staff?	Yes
		Are monthly management reports examined for variances against budget forecasts and such variances investigated?	Variance analaysis are carried out periodically.

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
12	**Internal Financial Controls**	Are wages/salaries independently checked against personnel records for unusual or excessive payments?	Yes
		Are duties segregated so that no individual can control any of the following activities from commencement to completion without referral to others; (a)signing cheques or authorising payments (including capital expenditure) above $5,000? (b)issuing funds transfer instructions? (c)amending funds transfer procedures? (d)opening new bank accounts or amending approved signatory details? (e)investment in and custody of securities and valuables (including blank cheques, travellers cheques, bills of exchange etc.)? (f)refund of monies or return of goods above $5,000? (g)disbursement of assets or funds of any Pension Plan? (h)appointing new suppliers or awarding contracts? (i)disbursement of loans (including loans to employees) or approving borrowings?	Yes
		Is all supporting documentation validated before signing cheques or authorising payments above $5,000?	Not Applicable, Payments are made through digital mode.
		Are statements of accounts sent to customers independently of employees receiving payment?	Yes
		Are bank statements independently reconciled by persons not authorised to deposit/withdraw funds, issue funds transfer instructions or dispatch accounts to customers, at least every 30 days?	Yes
12	**Recruitment Procedures**	When recruiting or promoting employees to positions of trust involving handling of stock, money, financial or treasury functions, do you: (a)obtain written references covering, at least, their previous 3 years employment history? (b)undergo a process to ensure their suitability for the position?	Corporation has recruitement policy and procedure which is in conformity with applicable Government regulations. Recruitment are carried out as per the policy either directly or through approved external agencies.
		Is there controlled access to all locations?	Yes
		Are all premises containing stock, money, securities, precious metals etc. connected to an intruder alarm which is connected to a central station or a police station and are such intruder alarms maintained in proper working order?	Not Applicable

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
13	**Stock and Physical Security**	Is an independent physical count of stock, raw materials, work in progress and finished goods undertaken at least quarterly and is this count reconciled against stock records?	Not Applicable
		Is the transfer of money and securities valued above $10,000 made by a security or professional cash carrying company?	Not Applicable
		What is the maximum value of money, securities, precious metals and/or jewellery at any one location: (a)during business hours?$ (b)outside business hours?$	Not Applicable
		What is the maximum value of stock, work-in-progress and raw materials at any one location?	Not Applicable
14	**Third Parties**	Do you maintain an approved suppliers list?	Yes
		Are suppliers and service providers: (a)vetted for competency, financial stability and honesty before being approved? (b)appointed under written contract?	Yes
		Are procedures in place to assess the suitability of trustees, fiduciaries, administrators or officers of all of your Pension Plans?	Yes
		(a)Do you outsource any normal administrative function to third party service providers? (b)If “yes”, please detail the services and estimated annual contract values.	No
		Do you audit outsourcing companies during the term of their contract?	No
		If the outsourcing company operates on your premises are their employees under your daily management control?	Yes
15	**Computer Systems / Internet E-Commerce**	Are unique passwords used to give various levels of entry to the computer depending on the users job functions?	Yes
		Are passwords automatically withdrawn when people leave?	Access rights are withdrwan immediately upon employee leaving the organisation.
		Are all amendments to programmes approved independently of the persons making the amendments?	Yes
		Are programmes protected to detect unauthorised changes?	Yes
		Is your computer system protected by virus detection and repair software?	Yes

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
		Which business activities do you utilise the Internet for? (i)E-Mail (ii)Advertising (iii)Selling Products (iv)Hosting Services for Third Parties (v)Other	Email and business applications.
		What is the estimated value of e-business revenue in your business?	Not applicable
		Please list your Website addresses	www.gicre.in
16	**Fund Transfers**	What is the approximate total annual value of fund transfers? (a)InterGroup Payments (b)External Payments	The Corporation's turnover for 2025-26 was Rs.53,948 Crore.
		Please specify which methods are utilised to send fund transfer instructions: (a)Type (b) Secured By (i)Written (i) Password (ii)Electronic (ii) Encryption (iii)Telephone (iii) Codeword (iv)Facsimile (iv) Callback	Fund transfers are carried out thorugh electronic mode as per instructions given by authorised signatories to Corporation's Banks. Fund transfers are also carried out through internet banking by authorised signatories following the maker-checker system and as per prescribed authority limits.
		Are all fund transfer instructions subject to a verification and authentication process?	Yes
		Can payment instructions only be made to accounts which are pre-determined as an approved beneficiary?	Yes
		Is the financial institution required to authenticate the instruction in accordance with a specified mandate before payment is released?	Yes
17	**Plans and Policies**	Do you maintain a written crisis management or contingency plan covering procedures following kidnapping or extortion?	Yes
		Do you maintain a written anti-fraud policy which is distributed throughout your organisation?	Yes
		Do you have a whistleblowing service accessible to all staff?	Yes
		Are special security precautions taken to protect against kidnapping of directors or employees who live in or travel to volatile countries?	Not applicable

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
18	**Optional Extensions to Cover**	(a)Theft (violent and forcible) of property from your premises by third parties? (b)Criminal damage (excluding fire) caused by any person? (i)CrimeManager Complete provides cover for your direct financial loss but please indicate whether you wish this to be extended to include (c)Contractual penalties incurred as a direct result of insured loss (d)Interest (prior to date of discovery) which would have been receivable or becomes payable as the direct result of insured loss?	Please refer to the Policy Coverage under Scope of work
19	**Loss History**	Please provide brief details of any losses (of a type covered by CrimeManager Complete) sustained during the past five (5) years and before application of any deductible, retention or excess whether insured or not.(Please include date discovered, location, nature of loss and amount).	(a) Natue of loss: Mail Spoofing incident (b) 13th April 2022 (c) Location : GIC Head Office (d) Amount: USD 326,500.70
		Please describe what corrective measures were taken to prevent similar losses.	Corrective measures taken include updating SOP of Accounts section with specific clause “Addition/Change of new/existing Banking details”
		Have such corrective measures been implemented across all operations?	Yes
	Crime Questionnaires		
1	**Compliance**	Have you implemented a procedure to permanently comply with all privacy relevant legislative statutory, regulatory and contractual requirements?	Yes; The Corporation has implemented organisation wide sensitivity labelling at document(office suite) and email (M365) level. Corporation has also implemented containerisation (Intune) and updated the information classifcation as per the data classification requirements.
		Do you have guidelines issued on the retention, storage, handling and disposal of records and information?	Yes
		Have you assigned a responsible person for providing guidance and ensuring awareness of privacy principles (e.g. Data Privacy Officer DPO)?	Yes
		Do you regularly scan critical systems (incl. penetration tests, vulnerability assessments) - either by yourself or supported by third party? What is the frequency of the scan conducted?	Yes
		What is the coverage of VAPT? When was the same last conducted? Was Log4shell and such, also included in the vapt scan conducted if not when would the same be conducted?	Q4 2025-26

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
2	**Information security aspects of business continuity management**	Have you conducted a Business Impact Analysis (BIA)? When was it last conducted?	Yes; It is being reviewed annually and the last review for BIA annual exercise was completed for 2025-26 in september 2025
		Do you have a board approved Business Continuity Management (BCM) plan in place that specifically addresses cyber incidents?	Yes; Board approved BCP Plan (v12.0) in in place. ISRMC approved Information security procedure V4.0 covers the cyber security & Cyber incidents specifically.
		Do you test your information security continuity plans (e.g. Business Continuity Management, Disaster Recovery) at least annually?	Yes; Business Continuity Management and Disaster Recovery tests are conducted annually.
		Are your information processing facilities (i.e. cyber systems, services or cyber infrastructure, or physical location housing it) implemented with redundancy?	Yes; GIC has an alternative location as Data Centre which provides redundancy of system services
		Please let us know how a typical BCP testing looks like in terms of Role played by different team and the process	Yes; Defined in BCP Procedural manual version 12.0
		Please explain in details. Please let us know how do you arrive at your RTO and RPO?	Yes; Different departments in the Organization has set of different parameters according to the relative processes. Business Impact Analysis (BIA) is documented and recorded accordingly & is reviewed annually. RTO is defined in BIA.
		What is the maximum acceptable outage or also known as RTO (Recovery Time Objective) for cyber systems? Please provide details on the same for critical and non critical systems.	Yes; The RTO is different for all critical business processes. Minimum RTO is 15 minutes and maximum is 30 days.
3	**Information security incident management**	Do you have board approved information security incident response plan in place?	Yes
		Do all your employees and third party providers know the reporting line / escalation procedure for information security events / incidents?	Yes
		Are employees and contractors required to report any identified information security weakness (not yet an incident or event) in systems or services?	Yes
		Do you use knowledge gained from analysing and resolving information security incidents to reduce the likelihood or impact of future information security incidents?	Yes
		Do you have segregation of network based on Business Function to avoid lateral spread?	Yes

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
		Are any data centers / networks / services being shared between the entities / subsidiaries to be covered / or even not covered under the policy please explain in detail?	No; Also please refer to the Scope of Cover
4	**Supplier relationships**	Have you identified and documented all your important suppliers / vendors (including third party service providers)?	Yes
		Do agreements with third party service providers require levels of security commensurate with your own information security standard?	Yes
		Do you monitor third party service provider / supplier activities for cyber security events to maintain an agreed level of information security?	Yes
5	**System acquisition, development and maintenance**	Does your web-server encrypt confidential data (e.g. HTTPS)?	Yes
		Do you test security functionality during the development lifecycle of information systems incl. IT security updates? If the response is no. request you to kindly share some more details on this aspect?	Yes
		Do you consider confidentiality when using operational data for testing to ensure that all sensitive details are protected by removal or modification?	Yes
6	**Communications security**	Are all internet access points secured by appropriately configured firewalls?	Yes
		Do you monitor your network and identify information security events?	Yes
		Are all internet-accessible systems (e.g. web-, email-servers) segregated from your trusted network (e.g. within a demilitarized zone (DMZ) or at a 3rd party provider)?	Yes
		Do you encrypt confidential communication (e.g. secure emails with SMIME (Secure Multipurpose Internet Mail Extensions) or SMTP-over-TLS (Simple Mail Transfer Protocol Secure))?	Yes

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
		Does the organization have network segregation implemented by isolating the demilitarized zone, InterVLAN communications, and Guest VLAN to prevent the movement of an attacker internally in case of a breach? Please explain intervlan security in detail?	Yes
7	**Operations security**	Have you implemented change management procedures for critical systems?	Yes
		Is the IT-environment for development and testing separated from production IT-environment?	Yes
		Do you use malware protection for all web-proxies, email-gateways, workstations and laptops?	Yes
		Besides traditional signature-based detection, does your malware protection use advanced heuristic- and behavioural-based detection mechanisms to protect against new malwares?	Yes
		Do you perform at least weekly regular backups of business critical data? Please explain in detail the backup strategy being used in the organisation?	Yes
		Do you produce and regularly review event logs recording user activities, exceptions, faults and information security events (at least from your firewalls and domain controller) ?	Yes
		Have you implemented a centralized software installation process?	Yes
		Do you timely – at least within one month of release – apply updates to critical IT-systems and applications ("security patching")? What is the update strategy followed in the organisation?	Yes; Critical IT systems and appplications are updated on priority basis.
		Do you technically or organisationally ensure that employees must not install and, or run unauthorised portable softwares on their workstations? (Please share the controls present excluding admin right restrictions being implemented)	Yes; Access to install/run unauthorised software is restricted.
8	**Physical and environmental security**	Do you maintain a list of personnel (employees, vendors and visitors) with authorized access to your premises and sensitive security areas?	Yes

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
9	**Cryptography**	Is all confidential information stored on mobile devices (e.g. smart phones, laptops) fully encrypted? If No, please elaborate.	Yes
		Have you developed and implemented a policy on the use, protection and lifetime of cryptographic keys?	Yes
10	**Access control**	Do you restrict employees and external users privileges on a business-need to know basis (particularly administrative permissions, access to sensitive data e.g. personal data, etc.)?	Yes
		Do you have a formal access provisioning process in place for assigning and revoking access rights?	Yes
		Do you prohibit local admin rights on workstations for employees?	Yes
		Do you review user access rights at least annually?	Yes
		Do you revoke all system access, accounts and associated rights after termination of users (incl. employees, temporary employees, contractors, vendors, etc.)?	Yes
		Have you implemented a password policy enforcing the use of long and complex passwords across your organisation? Long and complex passwords are defined as: eight characters or more; not consisting of words included in dictionaries; free of consecutive identical, all-numeric or all-alphabetic characters.	Yes
		Do you have PIM, PAM solution in place? If yes, please specify details including coverage of the solution being used?	Yes
		Is multi factor authentication being used for all the cyber systems & services? If no what is coverage of the same in the organisation?	Yes
		Are any of the manufacturing / logistic / generation systems / medical equipments. Either connected or dependant on IT systems which if not working might result in any loss?	Not Applicable
		Do you keep an up-to-date inventory of software (incl. operating systems) and hardware assets being used in the organisation?	Yes
		Do you classify information, data with regards to confidentiality?	Yes
		Are information labelling procedures implemented in accordance with the above information classification scheme?	Yes
		Do you provide guidance on how to handle classified information?	Yes

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
11	**Asset management**	Do you either restrict access to, or encrypt confidential information stored on removable media like external storage devices (e.g. USB sticks or hard disks)?	Yes
		Do you securely dispose media containing sensitive information if it is not used any longer or if it needs to be disposed?	Yes
		Do you have a comprehensive Configuration Management Database (CMDB) including: all IT assets, public cloud assets, dependencies, criticality, ownership, software and patch versions? If yes, is it in house or vendor solution - please provide details on the same?	Yes
12	**Human resource security**	Do you provide at least annual education to increase your users (employees and contractors) security awareness and prepare users to be more resilient and vigilant against phishing or cyber attacks?	Yes
		Do you have any User Behavioural Analytics tool (i.e. UEBA, etc.) to monitor patterns of human behaviour to detect anomalies from those patterns? Please explain in detail?	No
13	**Organization of information security**	Have you assigned a responsible person for information security (e.g. Chief Information Security Officer "CISO")?	Yes
		Do you have an up to date list of authorities and external contacts, which must be informed in case of an information security incident?	Yes
		Please list all the information security functions that exists (within the organization, via external vendor, MSP) to manage/perform day-to-day security tasks, functions (example: SOC, TI, IR, etc.)	Yes; SOC, SIEM/ SOAR, EDR, PIM/PAM, WAF, DLP, etc.
		Are any SaaS services being used, or provided? If yes who is responsible for the protection of data stored on the SaaS service? Please name the service provider being used?	Yes; Micorsoft 365
		Please share future plans / roadmap for improving cyber security architecture including time frames to implement if any?	Corporation ensures compliance with the Information and Cyber Security Guidelines isseud by IRDAI.
14	**Information security policies**	Have you documented and implemented a board approved information security policy which is corporate-wide and permanently available for all employees and relevant external parties?	Yes
		Has the organization documented and implemented a board approved cloud security policy to ensure cyber security requirements are catered to when utilizing cloud services for business?	Corporation has board approved Information Security Policy and the same is reviewed annually by external CERTin emplanelled consultatnt and updated taking into account changes in the applicbale regulatory guidelines.

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
		Please share the update strategy followed in the organisation? Does the organization have a patch management solution to ensure that all critical and high-risk vulnerabilities reported are patched or mitigated within stipulated timeline? For all IT systems and applications to prevent any known vulnerabilities being exploited?	Yes
		Does the organization timely, i.e. at least monthly, update IT systems and applications to prevent any known vulnerabilities being exploited? Or does the organization have a patch management solution to ensure that all critical and high-risk vulnerabilities reported are patched or mitigated within stipulated timeline?	Corporation carries out VAPT audit of its IT Systems and Web Appplications on quarterly basis and identified vulnerabilities are patched/addrssed as per requirement.
		Does the organization ensure that the default passwords on all computer systems (e.g. routers, etc) are changed to prevent entry in the organizations systems, networks through a brute force attack?	Yes
		Does the organisation ensure high availability of business critical cyber infrastructure to ensure business continuity in case of an cyber incident?	Yes
		Please elaborate in details. Does the organization have a Disaster Recovery (DR) site to allow it to continue business-sensitive operations in the event of any disaster? How many data centers does the organisation have? When was the last DR drill conducted?	Yes; Corporation has one DC and one DR at a remote location. DR drills are conducted periodically and last drill was conducted on 13th June 2026
		Does the organization have a dedicated or shared, Security Operations Center (SOC) either inhouse or outsourced that is capable of monitoring, reporting, investigating and recovering from any cyber security incident observed within the organization's cyber infrastructure?	Yes
		Does the organization have a Network Access Control (NAC) solution in place to allow the organization to restrict access to resources on their network and to prevent risk to the organization from internet of things (IoT), or weak access permissions, or advanced persistent threats (APT), etc?	Yes
		Has the organization implemented Deception Tool, or Honeypot solution to divert and detect attackers with no risk to real data, operations, or users?	Yes
		Has the organization implemented host-based firewall solution on end-user systems and servers to actively identify and mitigate malicious traffic incoming and outgoing from assets?	Yes
		Has the organization implemented an Endpoint threat Detection and Response (EDR) solution on all end point systems and servers to actively monitor and detect security threats based on system behaviour? Such as crowdstrike falcon EDR, etc.	Yes

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
15	**Technology implementation**	Has the organization implemented applications / softwares whitelisting solution on all end point systems and servers to restrict the use of only authorized applications / softwares on the assets? Please share controls present excluding admin right restrictions being implemented	Yes
		Has the organization implemented a Intrusion Detection and Prevention (IDS/IPS) solution for network, and host based on all end point systems to detect or prevent any malicious activity on IT assets by monitoring the network traffic?	Yes
		Has the organization implemented a Data Leakage Prevention (DLP) tool on all end point systems and servers in blocking mode for making sure that end users do not send sensitive or critical information outside the corporate network?	Yes
		Does the organization have a Next-Generation Firewall (NGFW) or Unified Threat Management (UTM) solution capable of in-line Deep Packet Inspection (DPI) and an Intrusion Prevention System (IPS) in place to reduce risks arising from network vulnerabilities?	Yes
		Does the organization ensure only secured connections like VPN are utilized by remote users to ensure the confidentiality of sensitive information in transit?	Yes
		Has the organization implemented a Security Incident and Event Management (SIEM) solution for proactively preventing, detecting, analyzing, and responding to security threats that the organization may face in a timely manner? Please provide coverage of the solution being used? Does it cover IT and OT assets?	Yes
		Has the organization implemented a Database Activity Monitoring (DAM) Solution to detect and prevent malicious behaviour in the database?	Yes
		Has the organization implemented anti-Distributed Denial-of-Service (DDoS) solution to prevent DDoS attacks?	Yes
		Please elaborate in details. What is the frequency of backup? How are backups taken? Please explain in detail the backup strategy & backup coverage being used in the organisation?	Yes; Daily incremental, weekly full, monthly full, yearly full
		Has the organization implemented anti-malware or equivalent protection on end-user devices and servers that are updated / patched as per the vendor's recommendations to prevent malicious software attacks (e.g. virus, ransomware, spyware, etc.)? When were they last updated to the latest software version available?	Yes; 4th June 2026
		Please describe your current status with regards to Zero trust architecture for your network? What are the ongoing projects towards ZTA?	Yes; We use ZTNA for remote access

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
		When were the WAF rules last updated? Were rules added to WAF solution, to prevent log4j vulnerabilities from being exploited? Please respond in details.	Rules are in place in WAF solution, to prevent log4j vulnerabilities from being exploited.
		Are any apache, or applications based on java being used in the organisation? When were all of the apache, or applications based on java last updated to the latest version available?	No
		Do you have a process of real time monitoring for Domain admin accounts? Kindly elaborate?	Yes
		Please describe your API security Framework?	Not Applicable

Cyber Risk Protector Supplemental Questionnaire - Ransomware

1	With respect to the Applicant’s efforts to mitigate phishing, select all that apply 1.Applicant provides security awareness training to employees at least annually. 2.Applicant uses simulated phishing attacks to test employees’ cybersecurity awareness at least annually. 3.Where the Applicant is conducting simulated phishing attacks, the success ratio was less than 15% on the last test (less than 15% of employees were successfully phished). 4. Applicant 'tags' or otherwise marks e-mails from outside the organization. 5.Applicant has a process to report suspicious e-mails to an internal security team to investigate.	1.Yes; 2.Yes; 3.Yes; 4.Yes; 5.Yes Additional Commentary on efforts to mitigate phishing: Phishing-resistant MFA & Advanced email filtering technologies has been implemented. Periodic cybersecurity awareness training based on functional roles are being provided to employees. Regular email alerts are also being sent to ensure employee awareness of cybersecurity. User awareness programs are being structured to sensitize executives, employees, and helpdesk personnel to high-risk impersonation and fraud scenarios.
2	Does the Applicant have a documented process to respond to phishing campaigns (whether targeted specifically at the Applicant or not)?	Yes
3	With respect to the Applicant’s efforts to block potentially harmful websites and/or email, select all that apply: 1.Applicant uses an e-mail filtering solution which blocks known malicious attachments and suspicious file types, including executables. 2.Applicant uses an e-mail filtering solution which blocks suspicious messages based on their content or attributes of the sender. 3.Applicant uses a web-filtering solution which stops employees from visiting known malicious or suspicious web pages. 4.Applicant uses block uncategorized and newly registered domains using web proxies or DNS filters. 5.Applicant uses a web-filtering solution which blocks known malicious or suspicious downloads, including executables. 6.Applicant’s e-mail filtering solution has the capability to run suspicious attachments in a sandbox. 7.Applicant’s web filtering capabilities are effective on all corporate assets, even if the corporate asset is not on a corporate network (e.g. assets are configured to utilize cloud-based web filters or require a VPN connection to browse the internet).	1.Yes 2.Yes 3.Yes 4.Yes 5.Yes 6.Yes 7.Yes

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
4	"With respect to authentication for employees who are remotely accessing the corporate network and any cloud-based services where sensitive data may reside (including VPN access, and cloud-based email and CRM; together 'remote access to corporate resources'), select the description which best reflects the Applicant's posture:(As used herein, "multi-factor authentication" means authentication which uses at least two different types of the possible authentication factors (something you know, something you have, and something you are); the Applicant can provide further explanation below)"		Multi-factor authentication is required by policy for all remote access to corporate resources; all exceptions to the policy are documented.
5	"With respect to authentication for independent contractors and vendors who are remotely accessing the corporate network and any cloud-based services where sensitive data may reside (including VPN access, and cloud-based email and CRM; together 'remote access to corporate resources'), select the description which best reflects the Applicant's posture: (The Applicant can provide further explanation below)"		Multi-factor authentication is required by policy for all remote access to corporate resources; all exceptions to the policy are documented.
6	"Does the Applicant's multifactor authentication implementation also meet the criteria that the compromise of any single device will only compromise a single authenticator? (For illustration: where authentication requires a password (knowledge) and a token (possession), this would not meet the criteria above if the token to prove possession is kept on a device the password is also entered into, exposing both if the device is compromised)"		Yes; the Applicant's multi-factor implementation meets the above criteria.
7	With respect to the Applicant's endpoint security of workstations (desktops and laptops), select all that apply: 1.Applicant's policy is that all workstations have antivirus with heuristic capabilities. 2.Applicant uses endpoint security tools with behavioral-detection and exploit mitigation capabilities. 3.Applicant has an internal group which monitors the output of endpoint security tools and investigates any anomalies.		1.Yes 2.Yes 3.Yes
8	With respect to monitoring the output of security tools, select the description which best reflects the Applicant's capabilities: (The Applicant can provide further explanation below)		Applicant has a 24/7 monitoring of security operations by a 3rd party (such as a Managed Security Services Provider).
9	What is the Applicant's average time to triage and contain security incidents of workstations year to date? (The Applicant can provide further explanation below)		30 minutes-2 hours
10	"With respect to access controls for each user's workstation, select the description which best reflects the Applicant's posture: (The Applicant can provide further explanation below)"		No employees are in the Administrators' group or have local admin access to their workstations.
11	With respect to protecting privileged credentials, select all that apply with respect to the Applicant's posture: 1.System administrators at the Applicant have a unique, privileged credential for administrative tasks (separate from their user credentials for everyday access, email, etc.). 2.Privileged accounts (including Domain Administrators) require multifactor authentication. 3.Privileged accounts are kept in a password safe that require the user to "check out" the credential (which is rotated afterwards). 4.There is a log of all privileged account use for at least the last thirty days. 5." Privileged Access Workstations (workstations that do not have access to internet or e-mail) are used for the administration of critical systems (including authentication servers/Domain Controllers)."		1.Yes 2.Yes 3.Yes 4.Yes 5.Yes

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
12	Indicate the Applicant's use of Microsoft Active Directory (across all domains/forests): (i)Number of user accounts in the Domain Administrators group (include service accounts - if any - in this total): (ii)"Number of service accounts in the Domain Administrators group: (""service account"" means a user account created specifically for an application or service to interact with other domain-joined computers):"		(i) 750 (ii) 50
13	"How many users have persistent privileged accounts for endpoints (servers and workstations)?(For the purposes of this question, “privileged accounts” means entitlements to configure, manage and otherwise support these endpoints; users who must ‘check out’ credentials should not be included. The Applicant can provide further explanation below)"		10
14	With respect to the security of externally facing systems, select all that apply to the Applicant’s posture: 1.Applicant conducts a penetration test at least annually to assess the security of its externally facing systems. 2.Applicant has a Web Application Firewall (WAF) in front of all externally facing applications, and it is in blocking mode. 3.Applicant uses an external service to monitor its attack surface (external/internet facing systems).		1.Yes 2.Yes 3.Yes
15	What is the Applicant’s target time to deploy ‘critical’ – the highest priority – patches (as determined by the Applicant’s standards for when patches must be deployed)?		Within 24 hours.
16	"What is the Applicant’s year to date compliance with its own standards for deploying critical patches? (The Applicant can provide further explanation below)"		>95%
17	With respect to the Applicant’s network monitoring capabilities, select all that apply: 1.Applicant uses a security information and event monitoring (SIEM) tool to correlate the output of multiple security tools. 2.Applicant monitors network traffic for anomalous and potentially suspicious data transfers. 3.Applicant monitors for performance and storage capacity issues (such as high memory or processor usage, or no free disk space). 4.Applicant has tools to monitor for data loss (DLP) and they are in blocking mode.		1.Yes 2.Yes 3.Yes 4.Yes
18	"With respecting to limiting lateral movement, select all that apply to the Applicant’s posture: (The Applicant can provide further explanation below)" 1.Applicant has segmented the network by geography (e.g. traffic between offices in different locations is denied unless required to support a specific business requirement). 2.Applicant has segmented the network by business function (e.g. traffic between asset supporting different functions – HR and Finance for example – is denied unless required to support a specific business requirement). 3.Applicant has implemented host firewall rules that prevent the use of RDP to log into workstations. 4.Applicant has configured all service accounts to deny interactive logons.		1.Yes 2.No 3.Yes 4.Yes
19	Enter the date of the Applicant’s last ransomware exercise; check the box if none has been conducted.		No ransomware exercise has been conducted.
20	Does the Applicant have a documented plan to respond to ransomware of a 3rd party provider/vendor or customer? If yes, please indicate principle steps.		No

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
21		"With regards to verifying the efficacy of security controls, select all that apply to the Applicant: (The Applicant can provide further explanation below)" 1.Applicant uses Breach and Attack Simulation (BAS) software to verify the effectiveness of security controls. 2.Applicant has an internal "red team" that tests security controls and response. 3.Applicant has engaged an external party to simulate threat actors and test security controls in the last year.	1.No 2.No 3.Yes Additional commentary on controls verification: As part of regulatory requirements, the corporation conducts quarterly VAPT and configuration assessments through an external CERT-In empanelled auditing firm.
22		With regards to disaster recovery capabilities, select all that apply to the Applicant: 1.A process for creating backups exists, but it is undocumented and/or ad hoc 2.Applicant has a documented Disaster Recovery Policy, including standards for backups based on information criticality. 3. At least twice a year, Applicant tests its ability to restore different critical systems and data in a timely fashion from its backups.	1.No 2.Yes 3.Yes
23	What is the Applicant's Recovery Time Objective (RTO) for critical systems?		< 4 hours
24		With respect to backup capabilities, select all that apply to the Applicant: 1.Applicant's backup strategy includes offline backups (can be stored on site) 2.Applicant's backup strategy includes offline backups stored offsite 3.Applicant's backups can only be accessed via an authentication mechanism outside of our corporate Active Directory.	1.Yes 2.Yes 3.Yes
25	Does the Applicant have a policy that all portable devices use full disk encryption?		Yes
26	**Data Security & Business Continuity**	Information security centrally managed for all operations	Yes
		Hardware inventory maintained and updated	Yes
		Daily asset discovery process	Yes
		Software inventory and support review	Yes
		Inventory of sensitive data stores	Yes
		Vital assets documented and prioritized	Yes
		RTO for vital assets	<5 hours
		Documented DR policy and backups	Yes
		Offline onsite backups	Yes
		Offline offsite backups	Yes
		Backups isolated from production domain	Yes
		Full disk encryption for endpoints with sensitive data	Yes
		Sensitive data at rest encrypted	Yes
		SOC/MSSP monitors vital assets	Yes
		SIEM used for vital asset logs	Yes
27		Microsoft AD used	Yes
		Azure AD used	Yes
		AD Federation Services used	Yes
		AD authoritative with Azure AD	Yes
		Inventory of user/admin accounts	Yes
		Annual account authorization review	Yes

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
	Identity, Credential, and Access Management Security	Password reuse awareness policy	Yes
		Separate admin credentials	Yes
		MFA for domain admins	Yes
		JIT privileged access	Yes
		30-day admin activity logs	Yes
		MFA for employee remote access	Yes
		MFA for vendor remote access	Yes
		MFA for SaaS vital assets	Yes
		Inventory maintained	Yes
		Passwords rotated annually	Yes
		Authenticator Assurance Level	AAL2
		No admin rights by default	Yes
		Persistent privileged users	10
		Domain controller logs to SIEM	Yes
28	Security Monitoring and Incident Response	24x7 MSSP monitoring	Yes
		SIEM correlation	Yes
		Network anomaly monitoring	Yes
		DLP in blocking mode	Yes
		Containment time	30 minutes-2 hours
		Vital assets logged to SIEM	>=71%
		External threat simulation	Yes
		Documented IR plan	Yes
		Phishing response process	Yes
29	Risk Management	Vulnerability scanning program	Yes
		Patching based on vital assets	Yes
		Threat intelligence considered	Yes
		Critical patch deployment target	Within 24 hours
		Patch compliance	>95%
		Social media restricted	Yes
		Personal email restricted	Yes
		Users report violations	Yes
		Monitor unauthorized remote access	Yes
		Monitor malicious sites/IPs	Yes
30	Phishing Defense	Annual awareness training	Yes
		Simulated phishing	Yes
		Success ratio <15%	Yes
		External email tagging	Yes
		Suspicious email reporting	Yes

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
30	Phishing Defense	Malicious attachment blocking	Yes
		Sender/content filtering	Yes
		Web filtering	Yes
		Block uncategorized domains	Yes
		Sandboxing capability	Yes
31	Malware Defense	AV with heuristics	Yes
		Behavioral detection	Yes
		EDR capabilities	Yes
		Application whitelisting	Yes
		All workstations/laptops covered	Yes
		All servers covered	Yes
		Daily updates	Yes
		Block malicious files	Yes
		Anti tamper enabled	Yes
		Network segmented by geography	Yes
		RDP restricted	Yes
		Service accounts deny logon	Yes
		Exercise in last year	No
32	Third Parties & Managed Service Providers Defense	MSP for security operations	Yes
		MSP for backup/recovery	Yes
		MSP for cloud transformation	Yes
		Persistent third-party access	Yes
		Third-party risk process	Yes
33	Perimeter and Internet Defense	Inventory of external assets	Yes
		Regular vulnerability scans	Yes
		WAF blocking mode	Yes
		External attack surface monitoring	Yes
		Ransomware-related ports blocked	Yes
		Threat detection and response	Yes

	Additional Questions	
1	Kindly confirm if coverages, limits and deductible mentioned in the tender are as per expiring policy.	Required modifications include 50% increase in cover limit over expiring policy. Please refer to Policy Coverage under Scope of Work.
2	Can GIC Re have any exposure through participating share in any Liability Domestic Treaty or by way of Obligatory under this policy.	No

General Insurance Corporation of India - Procurement of Cyber & Crime Insurance Policy 2026-27

GEM/2026/B/7923950

Responses to the Pre-bid queries received upto 19.08.2026

Q.No	Segment	Queries	GIC Re Clarification / Response
3	The tender document states coverages only, kindly share list of exclusions for the policy		Conditions & Exclusions: 1. Endorsement – OFAC Sanctions. 2. Exclusion for Outage of external network / Critical Infrastructure Failure Exclusion. 3. All other terms and conditions as per wordings. 4. Condition : No higher limits to be purchased without insurer's consent. 5. Endorsement – War, Cyber War and Cyber Operations Exclusion (LMA 5566). 6. Exclusion -Cryptocurrency Exclusion.
4	Kindly provide your response to following security measures: 1.Multi-factor authentication (MFA) mandatory for all users (at least 95% users) 2.Endpoint Detection and Response (EDR) tools deployed. (installed at least 95% devices) 3.Secure backups offsite storage 4.Regular software patching 5.Business Continuity Plans 6.Disaster Recovery Plans 7.Employee Security Awareness Training 8.Access controls with least privilege principles 9.Documented incident response plans		1.Yes 2.Yes 3.Yes 4.Yes 5.Yes 6.Yes 7.Yes 8.Yes 9.Yes