ZURICH kotak
General Insurance

ZURICH CYBER SOLUTIONS

Proposal Form – Extensive

(This Proposal Form is for organizations in the Large Corporate sector.)

GUIDELINES FOR COMPLETION OF THE PROPOSAL FORM

1. Please fill the proposal form in BLOCK LETTERS. All details with * are mandatory.
2. The Liability of the Company in relation to the subject matter of this Proposal does not commence until this Proposal has been accepted by the Company through the issuance of the Policy Document/Cover Note and subject to the receipt by the Company of the premium paid.
3. This Proposal will be the basis of any subsequent policy that we issue to you. It is therefore essential that you provide all the information in this Proposal FULLY, ACCURATELY AND CORRECTLY and that you provide us with any and all additional information relevant to risk to be insured or our decision as to acceptance of the risk or the terms upon which it should be accepted.
4. The Policy shall become voidable at the option of the Company, in the event of any untrue or incorrect or incomplete statement, misrepresentation, non-description or on non-disclosure in any material particular in the Proposal Form /personal statement, declaration and connected documents, or any material information having been withheld by the proposed policyholder or any one acting on its behalf to obtain any benefit under this Policy.
5. If you require additional space to answer any question on this Proposal Form, please attach additional sheets of paper and indicate on the additional sheet the question number to which the information being provided pertains. (Information given herein will be treated in strict confidence).

Policy issuing office:

Policy servicing office:

Intermediary/Agent Name:

Intermediary License no /Agent code.:

Intermediary/Agent Contact No.:

1. Name of Proposer: ____

Street Address: ____

City: ____

Website: ______________________________

2. Country of Registration: __________________________________

3. Date of incorporation/formation: ________________________

Additional Details:

Nationality: Indian ❑ Non – Indian ❑

If Non-Indian, please specify Country: …………………

Type of Organization

Corporations □ Governments□ Non Governmental Organizations □ Society □
International Organization □ Trust □ Partnership □ Cooperatives □ Section 25 Company □

Sources of funds: Please tick appropriate box
Salary □ Business □ Others (please specify)

---

4. Name of each entity to be included as an insured ____
____

How are these entities related to your business? ____
____

Proposer is: □ Corporation □ Partnership □ Individual

6. Year full time operation began: _____________

7. Limit(s) of Liability & Jurisdiction(s) being requested: ______________

8. Applicable Law:

9. Policy Period:

10. Territorial Scope of Cover required:

11. Retention (each Wrongful Act): __________

12. Revenue Details:

Revenue: Previous Year	
Revenue: Projected (Current Year)	
Revenue: Projected (Upcoming Year)	

Territory	**Percentage Split of Revenue**
Home Country	
UK	
Europe	
USA	
Australia/New Zealand	
Rest of the World	

13. No of Employees: ___________

No of IT Employees: ___________

No of Cybersecurity employees: _________

Company IT budget (annual): ___________

Cybersecurity budget (annual): __________

14. Has any other business been acquired, merged or consolidated with the applicant in the last two years? □Yes □ No

(if yes, please provide details below)

Company Name: _

Acquisition Date: ____

Turnover (Last 12 months):

Business activity different from acquiring company's:

____

____

____

Has all IT integration been completed? □Yes □ No
(if not, please provide details below):

____

____

____

15. Company's CKYC Identifier / Number (Generated by CERSAI):

PAN (mandatory):
GSTIN:

16. Please share the below details for the Authorised Signatory:

Name:
Designation:
PAN:
CKYC Identifier / Number (Generated by CERSAI):

17. Business Interruption

17.1. Internal Information Technology (IT) Systems:

How long can your business processes survive without critical internal IT systems?
□ All business processes can survive one week without critical internal IT systems.
□ Most business processes can survive at least one week without critical internal IT systems.
□ Most business processes can survive at least one day but less than one week without critical internal IT systems.
□ Most business processes can survive one day or not at all without critical internal IT systems.

What is the expected revenue effect if a critical internal IT system faces an interruption of:
24 hours:

□ Minimal impact expected if an internal IT system is interrupted for 24 hours.
□ Moderate impact expected if an internal IT system is interrupted for 24 hours.
□ Major impact expected if an internal IT system is interrupted for 24 hours.
Please fill in the estimated amount: _________________

7 days:

□ Minimal impact expected if an internal IT system is interrupted for 7 days.
□ Moderate impact expected if an internal IT system is interrupted for 7 days.
□ Major impact expected if an internal IT system is interrupted for 7 days.
Please fill in the estimated amount: _____________________

17.2 **Third Party IT Service Provider Information Technology (IT) Systems:**

How long can your business processes survive without outsourced critical IT systems?
□ All business processes can survive one week without critical external IT systems.
□ Most business processes can survive at least one week without critical external IT systems.
□ Most business processes can survive at least one day but less than one week without critical external IT systems.
□ Most business processes can survive one day or not at all without critical external IT systems.

What is the expected revenue effect if a critical IT supplier faces an interruption of:
24 hours:
□ Minimal impact expected if a critical IT provider is interrupted for 24 hours.
□ Moderate impact expected if a critical IT provider is interrupted for 24 hours.
□ Major impact expected if a critical IT provider is interrupted for 24 hours.
Please fill in the estimated amount:

7 days:
□ Minimal impact expected if a critical IT provider is interrupted for 7 days.
□ Moderate impact expected if a critical IT provider is interrupted for 7 days.
□ Major impact expected if a critical IT provider is interrupted for 7 days.
Please fill in the estimated amount:

17.3 Third Party Non-IT Service Provider Information Technology (IT) Systems:

How long can your business processes survive without access to an IT-System of a non-IT Service Provider
(e.g. your main supplier)?

□ All business processes can survive one week without access to IT-Systems of a non-IT Service Provider.
□ Majority of business processes can survive one week without access to IT-Systems of a non-IT Service Provider.
□ Majority of business processes can't survive days without access to IT-Systems of a non-IT Service Provider
□ Majority of business processes can't survive hours without access to IT-Systems of a non-IT Service Provider.

What is the expected revenue effect if a non-IT supplier faces an interruption of:
24 hours:

□ Minimal profit loss expected if a non-IT provider is interrupted for up to 24 hours.
□ Moderate profit loss expected if a non-IT provider is interrupted for up to 24 hours.
□ Major profit loss expected if a non-IT provider is interrupted for up to 24 hours.
Please fill in the estimated amount: _____________

7 days:

□ Minimal impact expected if a non-IT provider is interrupted for 7 days.
□ Moderate impact expected if a non-IT provider is interrupted for 7 days.
□ Major impact expected if a non-IT provider is interrupted for 7 days.
Please fill in the estimated amount: ___________

18. Industrial Sector (Tick box interface)

□ Accommodation and Food Services
□ Administrative and Support and Waste Management and Remediation Services
□ Agriculture, Forestry, Fishing and Hunting
□ Arts, Entertainment and Recreation
□ Construction
□ Educational Services
□ Energy
□ Finance and Insurance
□ Healthcare and Social Assistance
□ Information
□ Management of Companies and Enterprises
□ Manufacturing
□ Mining, Quarrying and Oil and Gas Extraction
□ Professional, Scientific and Technical Services
□ Public Administration
□ Real Estate and Rental and Leasing
□ Retail Trade
□ Transportation and Warehousing
□ Utilities
□ Wholesale Trade
□ Other:

Please give a short description of your business activity: ________________________

____

____

19. Data Exposure

19.1 How much personal or other protected data records do you collect, process or store?

	None	< 10'000	< 100'000	< 1 Mio	< 10 Mio	> 10 Mio
Personal Identifiable Information (PII)	□	□	□	□	□	□
Personal Health Information (PHI)	□	□	□	□	□	□
Personal Credit Card Information (PCI)	□	□	□	□	□	□
Other	□	□	□	□	□	□

19.2 Does the organization store, process or transmit government classified data? □Yes □ No

19.3 Does the organization store, process or transmit payment card data? □ Yes □ No

19.4 Does the organization use or provide technology that scans biometric identifiers (fingerprints, facial, voice, iris, etc.)? □ Yes □ No
19.5 Is the organization considered a Covered Entity under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act? □ Yes □ No

If there is any additional commentary on any specific question or response in this section, please provide below:
(please provide the number of the question you are referring to)

____

____

20. Outside Service Provider

What Cloud Service Provider does the organization use? Select all that all that apply:

□ Microsoft □ Google □Amazon
□ Other:

What key business processes/systems are outsourced to a third party? Select all that apply.

□ Microsoft 365 (Office + AD) Productivity Apps

□ Data Processing / Warehousing
□ Enterprise Resource Planning (ERP)
□ Disaster Recovery Services
□ Human Resources System
□ Payment and Transaction Processing
□ Customer Relationship Management (CRM)
□ Third-Party Risk Management (TPRM)
□ Managed Security Service (MSSP) / Security
□ Operations Center (SOC)
□ IT Operations
□ File Sharing
□ Other

Please list your critical IT, Cloud Service Providers and Business Process Outsourcers along with the services they provide
(e. g. Managed Security Services, Cloud/Backup/Website Hosting, Internet Service Providers, Business Critical Software Providers, Data Processors, Point-of-Sale (PoS) Hardware Providers, Colocation Services, Payment/Transaction Processing):

Provider	**Service**

If there is any additional commentary on any specific question or response in this section, please provide below:

21. Technology Exposure

21.1 Does the organization use and manage end user systems (laptops, desktops, mobile devices, tablets, etc.)? □Yes □ No

21.2 Does the organization use or manage terminals (ATMs, kiosks, payment terminals, etc.)? □Yes □ No

21.3 Does the organization use or manage removable media (USB storage devices, external hard drives, etc.)? □Yes □ No

21.4 Does the organization use or manage Healthcare Devices (including life support systems, insulin drips, health monitoring systems, etc.)? □Yes □ No

21.5 Does the organization use or manage critical Internet of Things (IoT) devices (door locks / actuators, smoke detectors, etc.)? □Yes □ No

21.6 Does the organization use or manage Operational Technology (OT, e.g. industrial machines, control systems, etc.)? □Yes □ No

If there is any additional commentary on any specific question or response in this section, please provide below:
(please provide the number of the question you are referring to)

22. Information Security Questionnaire

22.1 Organizational Governance

22.1.1 The organization maintains a formal Data/Cyber Security policy with defined procedures for all operations (ideally managed centrally). □ Yes □ No □Partially

22.1.2 A dedicated leadership role for cybersecurity is established (e.g. Chief Information Security Officer, CISO). This individual actively engages with key decision makers within the organization to prioritize and obtain approval for security initiatives. □ Yes □ No □Partially

22.1.3 A dedicated role for data protection is established in the company (Data Protection Officer, DPO/Chief Product Officer, CPO). □ Yes □ No □Partially

If there is any additional commentary on any specific question or response in this section, please provide below:
(please provide the number of the question you are referring to)

22.2 Cyber Risk Management Strategy and Processes

22.2.1 Security risk assessments are performed at least annually either internally or by an independent third party. □ Yes □ No □Partially

If there is any additional commentary on any specific question or response in this section, please provide below:

22.3 Compliance and Certifications

22.3.1 The organization has an active Information Security Management System (ISMS) certification (e.g. ISO27001). □ Yes □ No □Partially

22.3.2 The organization is required to be compliant with Payment Card Decision Support System (DSS) Standards (Payment Card Industry Data Security Standard, PCI-DSS). . □ Yes □ No □Partially

22.3.3 The company is Health Insurance Portability and Accountability Act (HIPAA) compliant and certified. □ Yes □ No □Partially

If there is any additional commentary on any specific question or response in this section, please provide below:
(please provide the number of the question you are referring to)

____

____

____

22.4 Asset Management

22.4.1 A centralized hardware inventory is maintained. □ Yes □ No □ Partially □ Yes, advanced
(If the inventory is automated using real-time discovery scanning, answer "yes, advanced")

7.4.2 A centralized software inventory is maintained. □ Yes □ No □ Partially □ Yes, advanced
(If the inventory is automated using real-time discovery scanning, answer "yes, advanced")

7.4.3 A centralized data inventory is maintained and data assets are labelled according to data classification standards. □ Yes □ No □ Partially □Yes, advanced
(If the inventory is automated using real-time discovery scanning, answer "yes, advanced")

7.4.4 A formal Business Impact Analysis (BIA) has been conducted within the last two years to understand the criticality and dependencies of all systems. □ Yes □ No □ Partially

7.4.5 Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are defined for critical systems and their dependent systems. □ Yes □ No □ Partially

Please specify on established time frames:

____

____

22.5 Supplier Management

22.5.1 Third parties with access to the organization's network and/or sensitive data undergo a risk assessment prior to onboarding and are subject to cybersecurity and liability contractual requirements. □ Yes □ No □ Partially

7.5.2 Critical third parties are monitored and audited periodically. □ Yes □ No □Partially
If there is any additional commentary on any specific question or response in this section, please provide below:
(please provide the number of the question you are referring to)

22.6 Identity and Access Management

22.6.1 Administrators have separate, privileged accounts for administrative tasks which are not used for internet and email access. □ Yes □ No □ Partially

7.6.2 Privileged accounts are tiered/unique for different system types (e.g. domain controllers, endpoints, servers, and applications). □ Yes □ No □ Partially

7.6.3 A Privileged Access Management (PAM) solution is deployed and/or access requires use of a Privileged Access Workstation (PAW). □ Yes □ No □ Partially

7.6.4 Multifactor Authentication (MFA) is enforced for all privileged accounts. □ Yes □ No □ Partially

7.6.5 Remote access to the corporate network is obtained through an encrypted channel (e.g. Virtual Private Network, VPN) and requires Multifactor Authentication (MFA).
□ Yes □ No □ Partially

7.6.6 Multifactor Authentication (MFA) is required for access to critical internet-facing applications.
□ Yes □ No □ Partially

7.6.7 Administrative Access rights are reviewed and recertified at least annually.
(If reviews are more frequent and/or a Privileged Access Management, PAM, tool is deployed, answer "yes, advanced") □ Yes □ No □ Partially □ Yes, advanced

7.6.8 Access rights are set up utilizing the "principle of least privilege". □ Yes □ No □ Partially

7.6.9 Local Administrator Accounts are centrally managed (e.g. using Local Administrator Password Solution, LAPS) and disabled by default on end user devices. □ Yes □ No □ Partially

7.6.10 Interactive login is denied for service accounts. □ Yes □ No □ Partially

7.6.11 Access to the backup environment requires non-Active Directory (AD) credentials and Multi-factor Authentication (MFA), or the use of credentials stored in a Privileged Access Management (PAM) solution. □ Yes □ No □ Partially

7.6.12 Privileged service account credentials are rotated at least annually.
(If a Privileged Access Management, PAM, tool is deployed and service accounts are onboarded, answer "yes, advanced") □ Yes □ No □ Partially □ Yes, advanced

If there is any additional commentary on any specific question or response in this section, please provide below:
(please provide the number of the question you are referring to)

22.7 Data Security

22.7.1 All backups are encrypted. □ Yes □ No □ Partially

22.7.2 Endpoint Data Loss Prevention (DLP) controls are implemented.
(If in blocking mode, answer "yes, advanced") □ Yes □ No □ Partially □ Yes, advanced

22.7.3 Multifactor Authentication (MFA) is required to access critical/sensitive information.
□ Yes □ No □ Partially

22.7.4 Development, testing and pre-production environments do not use live/sensitive data.
□ Yes □ No □ Partially

22.7.5 The company follows data retention and destruction procedures for all sensitive information.
□ Yes □ No □ Partially

22.7.6 Sensitive data at rest is encrypted using supported encryption protocols.
□ Yes □ No □ Partially

If there is any additional commentary on any specific question or response in this section, please provide below:
(please provide the number of the question you are referring to)

22.8 System Security

22.8.1 Critical business data is backed up daily. □ Yes □ No □ Partially
(if backups are weekly or less frequent, answer "partially")

22.8.2 Backups are stored offline and/or on a segmented network. □ Yes □ No □ Partially

22.8.3 All operating systems are hardened following recommended systems configurations
(e. g. Microsoft Security Baselines). □ Yes □ No □ Partially

22.8.4 Configuration assessment based on Center for Internet Security (CIS) benchmarks are regularily performed. □ Yes □ No □ Partially

If there is any additional commentary on any specific question or response in this section, please provide below:
(please provide the number of the question you are referring to)

22.9 Network and Communication Security

22.9.1 An email security solution is used to filter spam, phishing attempts, and malicious content.
□Yes □No □Partially

22.9.2 Sandboxing functionality is in place to inspect suspicious email attachments and links in an isolated test environment. □ Yes □ No □Partially

22.9.3 Malicious websites are blocked by a proxy/filter solution that is updated regularly.
□ Yes □ No □Partially

22.9.4 Firewalls and/or Intrusion Detection and Prevention Systems (IDS/IPS) are implemented to manage inbound/outbound network connections. □ Yes □ No □Partially

7.9.5 The organization's website and internet-facing systems are protected by a Web Application Firewall (WAF). (If the website is not used to generate revenue, answer "N/A".)
□ N/A □Yes □ No □ Partially

7.9.6 Adequate [1] Distributed Denial-of-Service (DDoS) prevention systems are in place.
(e.g. AWS Shield, Cloudflare, NETSCOUT Arbor DDoS Protection, etc.) □Yes □ No □ Partially

7.9.7 Access to corporate resources from personally owned devices (Bring Your Own Device, BYOD) is restricted or managed using a Mobile Device Management (MDM) solution. □Yes □ No □ Partially

7.9.8 Legacy/End-of-Life (EOL) assets are suitably segmented from the corporate network.
□ N/A □Yes □ No □ Partially

7.9.9 The network is segmented/micro-segmented using a risk-based approach (e.g. critical systems, sensitive data and critical/sensitive backups). □Yes □ No □ Partially

If there is any additional commentary on any specific question or response in this section, please provide below:
(please provide the number of the question you are referring to)

____

____

22.10 Operational Security

22.10.1 Monthly vulnerability scans are performed on internal network and connected systems.
□Yes □ No □ Partially

22.10.2 A centralized patch management is in place and patches are deployed within 30 days of release. Ideally, this is performed using an automated patching solution. □Yes □ No □ Partially

22.10.3 Emergency patching policy is followed for both Microsoft and non-Microsoft patches and deployed within three (3) days. □Yes □ No □ Partially

22.10.4 A reputable, vendor-supported advanced endpoint protection solution is installed on all endpoints and servers (e.g. CrowdStrike Falcon, SentinelOne EDR, Microsoft Defender or Endpoint or Cynet EDR). □Yes □ No □ Partially

22.10.5 Penetration testing is conducted annually on all critical external facing infrastructure. (If purple teaming is performed, answer "yes, advanced") □Yes □ No □ Partially □ Yes, advanced

22.10.6 End-of-Life (EOL) assets are segmented from the corporate network and extended support is purchased when available. □ N/A □ Yes □No □Partially

22.10.7 A Cloud Security Posture Management (CSPM) tool is implemented. □ Yes □ No □Partially

If there is any additional commentary on any specific question or response in this section, please provide below:
(please provide the number of the question you are referring to)

____

____

22.11 User Awareness and Training

22.11.1 Security awareness training is required for all employees and third parties with access to the corporate network upon hire and at least annually thereafter. □ Yes □No □Partially

The following solutions are considered adequate Distributed Denial-of-Service (DDoS) prevention systems (non-exhaustive):
- A solution from a telecommunications service provider;
- A solution from Microsoft or a cloud provider (if the company is hosted in the cloud or in a hybrid cloud);
- A dedicated solution from a Distributed Denial-of-Service (DDoS) protection provider.

22.11.2 Simulated phishing exercises are performed regularly. □ Yes □ No □Partially

Please specify frequency below:

____

____

If there is any additional commentary on any specific question or response in this section, please provide below:
(please provide the number of the question you are referring to)

____

____

22.12 Logging Events and Generating Alerts

22.12.1 A Security Information and Event Management (SIEM) solution is in place.

□Yes □ No □ Partially

22.12.2 The Security Information and Event Management (SIEM) tool is in place and ingests logs from most of the organization's assets and protective technologies (e.g. endpoints, servers, network devices, firewalls, Privileged Access Management, PAM, and Endpoint Detection and Response, EDR). □Yes □ No □ Partially □ Yes, advanced
(If the Security Information and Event Management, SIEM, ingests logs from over 80% of assets, answer "yes, advanced")

22.12.3 Threat intel is regularly collected and considered as part of the Security Operations Center (SOC) / Managed Detection and Response (MDR) (e. g. Indicators of Compromise, IOCs / Computer Emergency Response Team, CERT). □Yes □ No □ Partially

22.12.4 A 24 × 7 Security Operation Center (SOC) is established internally or outsourced to a third party (SOCaas/MDR). Analysts are able and authorized to contain and remediate potential security incidents upon detection. □Yes □ No □ Partially

22.12.5 The Organization has security tools (e.g. Endpoint Detection and Response, EDR or Security Information and Event Management, SIEM) that provide behavioral analytics.
□Yes □ No □ Partially

If there is any additional commentary on any specific question or response in this section, please provide below:
(please provide the number of the question you are referring to)

____

____

22.13 Response to Cyber Events

22.13.1 The organization has a documented Incident Response Plan (IRP).
□Yes □No □Partially

22.13.2 The Incident Response Plan (IRP) contains a ransomware scenario.
□ Yes □No □Partially

22.13.3 The organization has internal forensics specialists or forensics talent on retainer.
□Yes □No □Partially

22.13.4 Tabletop exercises to test the Incident Response Plan (IRP) and playbooks are performed at least annually and include key stakeholder participation. □Yes □No □Partially

If there is any additional commentary on any specific question or response in this section, please provide below:
(please provide the number of the question you are referring to)

____

____

22.14 Recovery from Cyber Events

22.14.1 The organization has a documented Disaster Recovery Plan (DRP) to guide recovery efforts following an incident or disaster. □ Yes □No □Partially

22.14.2 Recovery of all critical system backups is tested annually and meets Recovery Time Objectives (RTOs) / Recovery Point Objectives (RPOs). □ Yes □No □Partially

22.14.3 The organization has a documented Business Continuity Plan (BCP) to ensure continuation of critical business functions in the event of an incident or disaster. □ Yes □No □Partially

22.14.4 Tabletop exercises to test the Business Continuity Plan (BCP) are performed at least annually and include key stakeholder participation. □ Yes □No □Partially

22.14.5 The Organization scans backups for malware prior to restoration. □Yes □No □Partially

If there is any additional commentary on any specific question or response in this section, please provide below:
(please provide the number of the question you are referring to)

23 Supplemental Questionnaires

23.1 Operational Technology (OT)

23.1.1 The organization has a separate budget dedicated to Operational Technology (OT) cybersecurity
□N/A □Yes □No □Partially
.

23.1.2 A dedicated leadership role for Operational Technology (OT) cybersecurity is established.
□N/A □Yes □No □Partially

23.1.3 Remote access to Operational Technology (OT) assets is obtained through an encrypted channel (e.g. Virtual Private Network, VPN) and requires Multifactor Authentication (MFA).
□N/A □Yes □No □Partially

23.1.4 Segmentation is deployed between Operational Technology (OT) plants/facilities.
□N/A □Yes □No □Partially

23.1.5 A complete and up to date inventory of Operational Technology (OT) assets is maintained.
□N/A □Yes □No □Partially

23.1.6 Information Technology (IT) and Operational Technology (OT) environments are segmented.
□N/A □Yes □No □Partially

23.1.7 The Operational Technology (OT) environment is segmented from the internet.

□N/A □Yes □No □Partially

23.1.8 Vulnerability scanning of Operational Technology (OT) networks is performed regularly.
□N/A □Yes □No □Partially

23.1.9 Operational Technology (OT) assets are patched according to criticality. □N/A □Yes □No □Partially

23.1.10 Operational Technology (OT) logs are ingested by the Security Information and Event Management (SIEM). □N/A □Yes □No □Partially

23.1.11 The Operational Technology (OT) environment is monitored by the Security Operations Center (SOC). □N/A □Yes □No □Partially

23.1.12 An incident response tabletop exercise specific to Operational Technology (OT) cyber threats has been conducted within the last two (2) years. □N/A □Yes □No □Partially

23.1.13 Operational Technology (OT) systems are backed up at least monthly and when significant environment/process changes are made.

23.1.14 Restoration testing of Operational Technology (OT) systems backups is performed regularly. □N/A □Yes □No □Partially

23.1.15 A Business Contingency Plan (BCP) specific to Operational Technology (OT) is documented and has been updated within the last two (2) years. □N/A □Yes □No □Partially

23.2 Software Development

23.2.1 A secure Software/System Development Life Cycle (SDLC) is documented and includes standards for penetration testing, code analysis, User Acceptance Test (UAT), rollback plans, etc. The SDLC also prohibits the use of live/sensitive data in development, testing and pre-production environments. □N/A □Yes □No □Partially

23.2.2 Development, testing and pre-production environments are segmented from the corporate network. □N/A □Yes □No □Partially

23.3 Payment Card Industry Data Security (PCI-DSS)

23.3.1 The organization is Payment Card Industry (PCI)-certified at the appropriate level, based on the quantity of transactions processed per year. If a third-party payment processor is used, annual audit reports are obtained and reviewed to validate PCI-compliance.
□N/A □Yes □No □Partially

23.4 Health Insurance Portability and Accountability (HIPAA)

23.4.1 Personal Health Information (PHI) is protected and handled in accordance with the

Health Insurance Portability and Accountability Act (HIPAA) Security and Privacy rules.
□N/A □Yes □No □Partially

23.5 Biometric Data

23.5.1 Biometric data is adequately protected and the collection, processing, retention, storage, sharing, transferring, disposal, sale or other use of biometric data is in compliance with the applicable statute, rule, directive, ordinance, regulation, provision or common law governing the collection, confidentiality access, control, disclosure, retention, processing, modification, handling or use of biometric information.
□N/A □Yes □No □Partially

If there is any additional commentary on any specific question or response in this section, please provide below:
(please provide the number of the question you are referring to)

____

____

24 Applicant's History

24.1 In the past three years, has the applicant been declined any similar Cyber insurance or has the applicant's Insurer cancelled any previous Cyber insurance? □Yes □No

24.2 Has your company or any subsidiary experienced any system intrusion, business interruption, data theft or other data losses in the last five (5) years? □Yes □No

24.3 Are you or any other member of the Executive Board or management, aware of any circumstances (e. g. data breach) that could lead to a claim in connection with the insurance cover sought? □Yes □No

If yes, please provide details on incident date, description of incident(s), estimation of loss and/or costs, immediate
measures taken, and measures taken to prevent a similar loss?

____

____

BANK ACCOUNT DETAILS

<table>
<tr><th>PAYMENT DETAILS</th><th>REFUND / CLAIMS DETAIL</th></tr>
<tr><td>|__| Cheque |__| Demand Draft |__| Credit/Debit Card |__| Online Payment</td><td rowspan="2">|__| Details as per premium cheque to be used for electronic fund transfer; |__| Cancelled cheque submitted of other bank</td></tr>
<tr><td>Cheque / D.D # |__|__|__|__|__|__|__|__|__|__|</td></tr>
</table>

<table>
<tr><td>Drawn Amount
|__|__|__|__|__|__|__|__|__|__|__|__|__|</td><td>Account Number:
|____________________________|</td></tr>
<tr><td>Drawn To
|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__
|__|__|__|__|__|__|</td><td>IFSC/MICR Code:
|____________________________|</td></tr>
<tr><td>Date |__|__|__|__|__|__| |IFSC/MICR Code
|__|__|__|__|__|__|__|__|__|__|__|__|__|</td><td>Bank Name:
|____________________________|</td></tr>
<tr><td>Bank and Branch Name:</td><td>Account Holder name:
|__________________________|</td></tr>
<tr><td>For Credit/Debit Card:
Transaction Reference No:
|______________________________|
Transaction Date: |________________|</td><td><i>Disclaimer: Zurich Kotak General Insurance Company (India) Limited shall not be liable to anybody, in any manner, whatsoever if the NEFT transaction does not complete</i></td></tr>
</table>

ELECTRONIC INSURANCE ACCOUNT DETAILS OF PROPOSER (E-mail id is mandatory)

<table>
<tr><td>Do you have an EIA Account:</td><td>|__| Yes |__| No</td></tr>
<tr><td>If Yes, please quote EIA Number:</td><td></td></tr>
<tr><td>Please mention name of Insurance Repository:</td><td></td></tr>
<tr><td>If No, do you want Us to create an EIA account for you:</td><td>|__| Yes |__| No
(If Yes, please fill up Insurance Repository Application form)</td></tr>
<tr><td>Email id (Registered with Insurance Repository):</td><td></td></tr>
<tr><td colspan="2">Your address details as mentioned in the EIA account shall override the address provided in this application for Insurance.</td></tr>
</table>

- -

ACKNOWLEDGEMENT:

Received from Ms. /Mrs. / Mr. |__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__| a sum of Rs. |__|__|__|__|__|__|__|__|__| Through Cheque/DD |__|__|__|__|__|__|__|__|__| against your proposal for Zurich Cyber Solutions.

Signature of Zurich Kotak General Insurance Company (India) Limited Official / Intermediary|______________________|
Date |__|__|__|__|__|__|__|__|__|__|
Zurich Kotak General Insurance Company (India) Limited Official/Intermediary Name:
|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|
Time: |__|__|: |__|__| Place:

____

Note: Neither the submission of a completed proposal for insurance or any payment for any policy sought oblige the Company to agree to issue a policy, which decision is and always shall be in the Company's sole and absolute discretion. If Zurich Kotak General Insurance Company (India) Limited accepts a proposal for insurance, it shall be subject to the Board approved underwriting policy of Zurich Kotak General Insurance Company (India) Limited and the policy Terms and Conditions of Zurich Cyber Solutions and the Company shall have no liability to make any payment if premium is not received by Zurich Kotak General Insurance Company (India) Limited in full and in time, or is not realised. If a proposal is not accepted, Zurich Kotak General Insurance Company (India) Limited will inform you and refund any payment received from you without interest.

DECLARATION:

I / We hereby declare that the statements made by me / us in this Proposal Form are true to the best of my / our knowledge and belief and I / We hereby agree that this declaration shall form the basis of the contract between me / us and the "Zurich Kotak General Insurance Company (India) Limited"

Protect and contribute in conserving the environment, all your policy and service related communication would be sent in soft copy to the email id mentioned in the proposal form and it is valid for all regulatory /policy servicing requirements. |__| I / We would still want to receive a physical copy of the policy.

|__| I / We hereby give my/our consent to the Company to verify and obtain my/our identity/address proof through Central KYC Registry or Goods and Service Tax Portal or Ministry Of Corporate Affairs Portal or National Securities Depository Limited portal for the purpose of undertaking KYC.

AML DECLARATION

I / We hereby confirm that all premiums have been/will be paid from bonafide sources and no premiums have been /will be paid out of proceeds of crime related to any of the offence listed in Prevention of Money Laundering Act,2002. I / We understand that the Company has the right to call for document to establish sources of funds. The Insurance Company has right to cancel the insurance contract in case I am/have been found guilty by any competent court of law under any of the statutes, directly or indirectly governing the prevention of money laundering in India.

In case of entity, Type of Organization making the payment:

|__| Limited Company |__| Government Organization |__| Non-Government Organization (NGO) |__|
Society |__| Trust |__| Partnership |__| International Organization |__|
Co-operatives |__| Section 25 Company |__| Others

Are You or any of the proposed applicants or close relatives is/are associated to Politically Exposed Person (PEP)?* |__| Yes |__| No

"Politically Exposed Persons" (PEPs) are individuals who have been entrusted with prominent public functions by a foreign country, including the heads of States or Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.

Are you a Non-Profit Organization?* (only in case of an entity) |__| Yes |__| No

"Non-profit organization" means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a

Company registered under the section 8 of the Companies Act, 2013 (18 of 2013)."

*Place: ____________________________

*Date: |__|__| / |__|__| / |__|__|__|__|

*Signature and Stamp of Proposer

DECLARATION FOR AGENT

I hereby declare that, I have fully explained the features and terms & condition of the policy in detail to the Proposer and the Proposer has affixed the signature after fully understanding the features thereof.

Signature of Proposer

Signature & Stamp as applicable of the Insurance Advisor/ Specified person of Corporate Agent/Authorised Employee of Broker/ Sales person*

*Place: ________________________

*Date: |__|__| / |__|__| / |__|__|__|__|

VERNACULAR DECLARATION:

I hereby declare that, I have fully explained the contents of the proposal form and terms and conditions of the Policy to the Proposer in the language understood to him/her and that the Proposer has affixed the thumb impression / signature above after fully understanding the contents thereof.

Signature of Proposer

Signature of Intermediary/ Sales Person*

*Place: ____________________________

*Date: |__|__| / |__|__| / |__|__|__|__|

STATUTORY WARNING

PROHIBITION OF REBATES (Under Section 41 of Insurance Act 1938)

1) No person shall allow or offer to allow, either directly or indirectly as an inducement to any person to take out or renew or continue an insurance in respect of any kind of risk relating to lives or property, in India, any rebate of the whole or part of the commission payable or any rebate of the premium shown on the Policy, nor shall any person taking out or renewing or continuing a Policy accept any rebate, except such rebate as may be allowed in accordance with the published prospectuses or tables of the Insurer.
2) Any person making default in complying with the provisions of this section shall be punishable with fine, which may extend to Ten Lakhs Rupees.