CYBER APPLICATION FORM

PLEASE NOTE: This application will need to be signed and dated within 30 days of of the policy inception date (within 60 days for renewal policies).

BASIC COMPANY DETAILS

Please complete the following details for the entire company or group (including all subsidiaries) that is applying for the insurance policy:

Company Name: **Primary Industry Sector:**

Physical Address:

Description of Business Activities:

Website Address:

Date Established (mm/dd/yyyy): **Number of Employees:**

Last Complete Financial Year Gross Revenue: $ **Gross Revenue from International Sales: $**

Please state which financial institution(s) you use for commercial banking:

PRIMARY CONTACT DETAILS

To allow us to provide risk management alerts and updates, please provide contact details for the most relevant person within your organization for receiving such updates:

Contact Name: **Position:**

Email Address: **Telephone Number:**

BASIC RISK QUESTIONS

Please confirm whether multi-factor authentication is always enabled on all email accounts: ☐ **Yes** ☐ **No**

Do you maintain daily offline backups of all critical data? ☐ **Yes** ☐ **No**

Is any part of your IT infrastructure outsourced to third party technology providers, including application service providers? ☐ **Yes** ☐ **No**

If you answered yes to the question above, please list your most critical third party technology providers below (up to a maximum of 10):

PREVIOUS CYBER INCIDENTS

Please tick all the boxes below that relate to any cyber incident that you have experienced in the last five years (there is no need to highlight events that were successfully blocked by security measures):

☐ **Cyber Crime** ☐ **Cyber Extortion** ☐ **Data Loss** ☐ **Denial of Service Attack**

☐ **IP Infringement** ☐ **Malware Infection** ☐ **Privacy Breach** ☐ **Ransomware**

☐ **Other (Please Specify):**

If you ticked any of the boxes above, did the incident(s) have a direct financial impact upon your business of more than $10,000? ☐ **Yes** ☐ **No**

If you have experienced a previous cyber incident, please provide full details of the incident, the financial impact, and the measures taken since to prevent the incident from occurring again:

SUPPLEMENTARY QUESTIONS

Please Note: These supplementary questions help us to obtain a more complete picture of your company and the security controls you have in place. We request you answer all questions to the best of your ability and in some circumstances, we may require you answer all questions before we can issue a quote.

REVENUE ANALYSIS

Please complete the answers to the questions below. Where you do not have the exact information available please provide the closest approximation and indicate that you have taken this approach.

Please provide the following details for your top 5 clients:

Client Name	Primary Services	% of Insured's Revenue Generated From Client

IT RESOURCING AND INFRASTRUCTURE

What was your approximate operational expenditure on IT security in the last financial year? (including salaries, annual licenses, consultancy costs, etc.):

What was your approximate capital expenditure on IT security in the last financial year? (including hardware, one off software costs, etc.):

Do you anticipate spending more, the same or less in this financial year?

Is your IT infrastructure primarily operated and managed in-house or outsourced?

How many full-time employees do you have in your IT department?

How many of these employees are dedicated to a role in IT security?

INFORMATION SECURITY GOVERNANCE

Who is responsible for IT security within your organisation (by job title)?

How many years have they been in this position within your company?

Please describe the type, nature and volume of the data stored on your network:

Please describe your data retention policy:

Do you comply with any internationally recognized standards for information governance (if yes, which ones):

CYBER SECURITY CONTROLS

If your organization uses Remote Desktop Protocol (RDP) to allow remote access to your network, please describe the measures you adopt to secure it:

Please describe your process for patching all operating systems and applications:

How often do you conduct vulnerability scanning of your network perimeter?

How often do you conduct penetration testing of you network architecture?

Please provide details of the third party providers you use to conduct penetration testing:

Please describe your data backup procedures:

Please tick all the boxes below that relate to controls that you currently have implemented within your IT infrastructure (including where provided by a third party). If you're unsure of what any of these tools are, please refer to the explanations on the final page of this document.

- ☐ **Advanced Endpoint Protection**
- ☐ **Application Whitelisting**
- ☐ **Asset Inventory**
- ☐ **Custom Threat Intelligence**
- ☐ **Database Encryption**
- ☐ **Data Loss Prevention**
- ☐ **DDoS Mitigation**
- ☐ **DMARC**
- ☐ **DNS Filtering**
- ☐ **Employee Awareness Training**
- ☐ **Incident Response Plan**
- ☐ **Intrusion Detection System**
- ☐ **Mobile Device Encryption**
- ☐ **Penetration Tests**
- ☐ **Perimeter Firewalls**
- ☐ **Security Info & Event Management**
- ☐ **Two-factor Authentication**
- ☐ **Vulnerability Scans**
- ☐ **Web Application Firewall**
- ☐ **Web Content Filtering**

Please provide the name of the software or service provider that you use for each of the controls highlighted above:

IMPORTANT NOTICE

By signing this form, you agree that the information provided is both accurate and complete and that you have made all reasonable attempts to ensure this is the case by asking the appropriate people within your business. Evolve MGA will use this information solely for the purposes of providing insurance services and may share your data with third parties in order to do this. We may also use anonymized elements of your data for the analysis of industry trends and to provide benchmarking data.

Contact Name: **Position:**

Signature: **Date (mm/dd/yyyy):**

Cyber security controls explained

Advanced endpoint protection

Software installed on individual computers (endpoints) that uses behavioural and signature based analysis to identify and stop malware infections.

Application whitelisting

A security solution that allows organisations to specify what software is allowed to run on their systems, in order to prevent any nonwhitelisted processes or applications from running.

Asset inventory

A list of all IT hardware and devices an entity owns, operates or manages. Such lists are typically used to assess the data being held and security measures in place on all devices.

Custom threat intelligence

The collection and analysis of data from open source intelligence (OSINT) and dark web sources to provide organisations with intelligence on cyber threats and cyber threat actors pertinent to them.

Database encryption

Where sensitive data is encrypted while it is stored in databases. If implemented correctly, this can stop malicious actors from being able to read sensitive data if they gain access to a database.

Data loss preventions

Software that can identify if sensitive data is being exfiltrated from a network or computer system.

DDoS mitigation

Hardware or cloud based solutions used to filter out malicious traffic associated with a DDoS attack, while allowing legitimate users to continue to access an entity's website or web-based services.

DMARC

An internet protocol used to combat email spoofing – a technique used by hackers in phishing campaigns.

DNS filtering

A specific technique to block access to known bad IP addresses by users on your network.

Employee awareness

Training programmes designed to increase employees' security awareness. For example, programmes can focus on how to identify potential phishing emails.

Incident response plan

Action plans for dealing with cyber incidents to help guide an organisation's decision-making process and return it to a normal operating state as quickly as possible.

Intrusion detection system

A security solution that monitors activity on computer systems or networks and generates alerts when signs of compromise by malicious actors are detected.

Mobile device encryption

Encryption involves scrambling data using cryptographic techniques so that it can only be read by someone with a special key. When encryption is enabled, a device's hard drive will be encrypted while the device is locked, with the user's passcode or password acting as the special key.

Penetration tests

Authorized simulated attacks against an organisation to test its cyber security defences. May also be referred to as ethical hacking or red team exercises.

Perimeter firewalls

Hardware solutions used to control and monitor network traffic between two points according to predefined parameters.

Security info & event management (SIEM)

System used to aggregate, correlate and analyse network security information – including messages, logs and alerts – generated by different security solutions across a network.

Two-factor authentication

Where a user authenticates themselves through two different means when remotely logging into a computer system or web based service. Typically a password and a passcode generated by a physical token device or software are used as the two factors.

Vulnerability scans

Automated tests designed to probe computer systems or networks for the presence of known vulnerabilities that would allow malicious actors to gain access to a system.

Web application firewall

Protects web facing servers and the applications they run from intrusion or malicious use by inspecting and blocking harmful requests and malicious internet traffic.

Web content filtering

The filtering of certain web pages or web services that are deemed to pose a potential security threat to an organisation. For example, known malicious websites are typically blocked through some form of web content filtering.