

INSURING COMMUNITIES

COMPANY INFORMATION

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

Company Name: _____ Last Year's Gross Revenue: \$ _____

Website: _____ Date Established: M M / D D / Y Y Y Y

Physical Address of Headquarters: _____

Primary Industry Sector & Description of Business Activities: _____

INFORMATION SECURITY GOVERNANCE

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:

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? If it is outsourced, who do you outsource it to?

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?

Who is responsible for IT security within your organization (by job title)? How many years have they been in this position within your company?

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

CLOUD SERVICE PROVIDERS

Please tick all the boxes below that relate to companies or services where you store sensitive data or who you rely upon to provide critical business services:

- | | | | |
|-------------------------------------|--|--|---------------------------------------|
| <input type="checkbox"/> Adobe | <input type="checkbox"/> Amazon Web Services | <input type="checkbox"/> Dropbox | <input type="checkbox"/> Google Cloud |
| <input type="checkbox"/> IBM | <input type="checkbox"/> Microsoft 365 | <input type="checkbox"/> Microsoft Azure | <input type="checkbox"/> Oracle Cloud |
| <input type="checkbox"/> Salesforce | <input type="checkbox"/> Salesforce | <input type="checkbox"/> SAP | <input type="checkbox"/> Workday |

CYBER INSURANCE SUPPLEMENTARY FORM

CYBER SECURITY CONTROLS

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.

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

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

PREVIOUS CYBER INCIDENTS

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

<input type="checkbox"/> Cyber Crime	<input type="checkbox"/> Cyber Extortion	<input type="checkbox"/> Data Loss	<input type="checkbox"/> Denial of Service Attack	<input type="checkbox"/> IP Infringement
<input type="checkbox"/> Malware Infection	<input type="checkbox"/> Privacy Breach	<input type="checkbox"/> Ransomware	<input type="checkbox"/> 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 yes, please provide more information below, including details of the financial impact and measures taken to prevent the incident from occurring again:

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 INSURANCE SUPPLEMENTARY FORM

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 organizations to specify what software is allowed to run on their systems, in order to prevent any non-whitelisted 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 organizations 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 PREVENTION

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 addresses by users on your network.

EMPLOYEE AWARENESS

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

INCIDENT RESPONSE PLAN

Action plans for dealing with cyber incidents to help guide an organization'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 organization 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 users authenticate 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 organization. For example, known malicious websites are typically blocked through some form of Web Content Filtering.