Proposal Form

CyberEdge® Ransomware

This Supplemental Questionnaire is applicable to CyberEdge® coverage. As used herein, "**Applicant**' includes the **Policyholder** applying for CyberEdge® coverage and its subsidiaries.

Full Name of Applicant

1. With respect to the Applicant's efforts to mitigate phishing, **select all that apply:**
   - ☐ Applicant provides security awareness training to employees at least annually.
   - ☐ Applicant uses simulated phishing attacks to test employees' cybersecurity awareness at least annually.
   - ☐ 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).
   - ☐ Applicant 'tags' or otherwise marks e-mails from outside the organisation.
   - ☐ Applicant has a process to report suspicious e-mails to an internal security team to investigate.
   - ☐ None of the above.

   Additional Commentary on efforts to mitigate phishing:

2. Does the Applicant have a documented process to respond to phishing campaigns (whether targeted specifically at the Applicant or not)? ☐ Yes ☐ No

   If "Yes", please describe the principal steps to respond:

3. With respect to the **Applicant's** efforts to block potentially harmful websites and/or email, **select all that apply**:
   - ☐ **Applicant** uses an e-mail filtering solution which blocks known malicious attachments and suspicious file types, **including executables**.
   - ☐ **Applicant** uses an e-mail filtering solution which blocks suspicious messages based on their content or attributes of the sender.
   - ☐ **Applicant** uses a web-filtering solution which stops employees from visiting known malicious or suspicious web pages.
   - ☐ **Applicant** uses block uncategorized and newly registered domains using web proxies or DNS filters.
   - ☐ **Applicant** uses a web-filtering solution which blocks known malicious or suspicious downloads, **including executables**.
   - ☐ **Applicant's** e-mail filtering solution has the capability to run suspicious attachments in a sandbox.
   - ☐ **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).
   - ☐ None of the above.

   Additional commentary on efforts to block malicious websites and/or email:

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)

   - ☐ Remote access to corporate resources requires a valid username and password (single factor authentication).
   - ☐ Multi-factor authentication is in place for some types of remote access to corporate resources, but not all.
   - ☐ Multi-factor authentication is required by policy for all remote access to corporate resources; all exceptions to the policy are documented.
   - ☐ **Applicant** does not provide remote access to employees.

   Additional commentary on authentication for employees:

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)

   - ☐ Remote access to corporate resources requires a valid username and password (single factor authentication).
   - ☐ Multi-factor authentication is in place for some types of remote access to corporate resources, but not all.
   - ☐ Multi-factor authentication is required by policy for all remote access to corporate resources; all exceptions to the policy are documented.
   - ☐ **Applicant** does not provide remote access to independent contractors/vendors.

   Additional commentary on authentication for independent contractors/vendors:

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)

   - ☐ Not Applicable (**Applicant** does not use multi-factor authentication)
   - ☐ No; **Applicant's** multi-factor implementation does not meet the above criteria.
   - ☐ Yes; the **Applicant's** multi-factor implementation meets the above criteria.

   Additional commentary on Multi-factor authentication implementation:

7. With respect to the **Applicant's** endpoint security of workstations (desktops and laptops), **select all that apply**:
   - ☐ **Applicant's** policy is that all workstations have antivirus with heuristic capabilities.
   - ☐ **Applicant** uses endpoint security tools with behavioral-detection and exploit mitigation capabilities.
   - ☐ **Applicant** has an internal group which monitors the output of endpoint security tools and investigates any anomalies.
   - ☐ None of the above.

   Additional commentary on endpoint security capabilities:

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** does not have staff dedicated to monitoring security operations (a "**Security Operations Center**").
   - ☐ **Applicant** has a **Security Operations Center,** but it's not 24/7 (can be internal or external).
   - ☐ **Applicant** has a 24/7 monitoring of security operations by a 3rd party (such as a Managed Security Services Provider).
   - ☐ **Applicant** has 24/7 monitoring of security operations internally.

   Additional commentary on security monitoring:

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)
   - ☐ **Applicant** does not track this metric/Do not know
   - ☐ <30 minutes
   - ☐ 30 minutes-2 hours
   - ☐ 2-8 hours
   - ☐ >8 hours

   Additional commentary on average time to remediate:

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.
    - ☐ **Applicant's** policy is that employees by default are not in the Administrators' group and do not have local admin access; all exceptions to the policy are documented.
    - ☐ Some of **Applicant's** employees are in the Administrators' group or are local admins.
    - ☐ Do not know.

    Additional commentary on access controls for workstations:

11. With respect to protecting privileged credentials, **select all that apply** with respect to the **Applicant's** posture:
    - ☐ System administrators at the **Applicant** have a unique, privileged credential for administrative tasks (separate from their user credentials for everyday access, email, etc.).
    - ☐ Privileged accounts (including Domain Administrators) require multifactor authentication.
    - ☐ Privileged accounts are kept in a password safe that require the user to "check out" the credential (which is rotated afterwards).
    - ☐ There is a log of all privileged account use for at least the last thirty days.
    - ☐ 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).
    - ☐ None of the above.

    Additional commentary on protecting privileged credentials:

12. Indicate the **Applicant's** use of Microsoft Active Directory (across all domains/forests):

    Applicant does not use Microsoft Active Directory ☐ Yes ☐ No

    Number of user accounts in the Domain Administrators group (include service accounts - if any - in this total):

    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)

    Additional commentary on the number of Domain Administrators:

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)

    Please enter an integer:

    Additional commentary on the number of privileged accounts:

14. With respect to the security of externally facing systems, **select all that apply** to the **Applicant's** posture:
    - ☐ **Applicant** conducts a penetration test at least annually to assess the security of its externally facing systems.
    - ☐ **Applicant** has a Web Application Firewall (WAF) in front of all externally facing applications, **and it is in blocking mode**.
    - ☐ **Applicant** uses an external service to monitor its attack surface (external/internet facing systems).
    - ☐ None of the above.

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)?
    - ☐ There is no defined policy for when patches must be deployed.
    - ☐ Within 24 hours
    - ☐ 24-72 hours
    - ☐ 3-7 days
    - ☐ > 7 days

    Additional commentary on target times for patching:

16. What is the **Applicant's** year to date compliance with its own standards for deploying critical patches?
    - ☐ **Applicant** does not track this metric/Do not know
    - ☐ >95%
    - ☐ 90-95%
    - ☐ 80-90%
    - ☐ <80%

    Additional commentary on patching compliance:

17. With respect to the **Applicant's** network monitoring capabilities, **select all that apply**:
    - ☐ **Applicant** uses a security information and event monitoring (SIEM) tool to correlate the output of multiple security tools.
    - ☐ **Applicant** monitors network traffic for anomalous and potentially suspicious data transfers.
    - ☐ **Applicant** monitors for performance and storage capacity issues (such as high memory or processor usage, or no free disk space).
    - ☐ **Applicant** has tools to monitor for data loss (DLP) and they are in **blocking mode**.
    - ☐ None of the above.

    Additional commentary on network monitoring:

18. With respecting to limiting lateral movement, **select all that apply** to the **Applicant's** posture:
    (The Applicant can provide further explanation below)
    - ☐ **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).
    - ☐ **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).
    - ☐ **Applicant** has implemented host firewall rules that prevent the use of RDP to log into workstations.
    - ☐ **Applicant** has configured all service accounts to deny interactive logons.
    - ☐ None of the above.

    Additional commentary on segmentation:

19. Enter the date of the **Applicant's** last ransomware exercise; check the box if none has been conducted.

    Date: / / ☐ 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. ☐ Yes ☐ No

    3rd party ransomware response principle steps:

21. With regards to verifying the efficacy of security controls, **select all that apply** to the **Applicant**: (The Applicant can provide further explanation below)

    ☐ **Applicant** uses Breach and Attack Simulation (BAS) software to verify the effectiveness of security controls.
    ☐ **Applicant** has an internal "red team" that tests security controls and response.
    ☐ **Applicant** has engaged an external party to simulate threat actors and test security controls in the last year.
    ☐ None of the above.

    Additional commentary on controls verification:

22. With regards to disaster recovery capabilities, **select all that apply** to the **Applicant**:

    ☐ A process for creating backups exists, but it is undocumented and/or ad hoc
    ☐ **Applicant** has a documented Disaster Recovery Policy, including standards for backups based on information criticality.
    ☐ At least twice a year, **Applicant** tests its ability to restore different critical systems and data in a timely fashion from its backups.
    ☐ None of the above.

23. What is the **Applicant's** Recovery Time Objective (RTO) for critical systems?

    ☐ **Applicant** does not have an RTO/Does not know
    ☐ < 4 hours
    ☐ 4-24 hours
    ☐ 1 to 2 days
    ☐ 2-7 days

24. With respect to backup capabilities, **select all that apply** to the **Applicant**:

    ☐ **Applicant's** backup strategy includes offline backups (can be stored on site)
    ☐ **Applicant's** backup strategy includes offline backups stored offsite
    ☐ **Applicant's** backups can only be accessed via an authentication mechanism outside of our corporate Active Directory.

    Additional commentary on backup capabilities:

25. Does the **Applicant** have a policy that all portable devices use full disk encryption? ☐ Yes ☐ No

    Additional commentary:

This Supplemental Questionnaire is incorporated into and made part of any Application for CyberEdge® coverage by the **Applicant**. All representations and warranties made by **Applicant** in connection with such Application also apply to the information provided in this Supplemental Questionnaire.

Should the insurer issue a policy, the **Applicant** agrees that such policy is issued in reliance upon the truth of the statements and representations in this Supplemental Questionnaire or incorporated by reference herein. Any misrepresentation, omission, concealment or incorrect statement of a material fact, in this Supplemental Questionnaire, incorporated by reference or otherwise, may entitle the insurer to rescind the contract, refuse to pay a claim or reduce the amount it will be liable to pay in respect of a claim.

The undersigned hereby agrees, warrants, and represents that he or she is a duly authorized representative of the **Applicant**, and is fully authorized to answer and make statements and representations by and on behalf of the **Applicant**.

Signed

(Duly authorized representative, by and behalf of the **Applicant**)

Date / /

Title

Organisation

(Organisation's seal)

Important Notices

This Policy is issued/insured by AIG Australia Limited (AIG), ABN 93 004 727 753 AFSL No 381686

Sydney: 2 Park Street, NSW 2000 (1300 030 886)
Melbourne: Level 13, 717 Bourke Street, VIC 3008 (1300 030 886)
Brisbane: 10 Eagle Street, QLD 4000 (1300 030 886)
Perth: 77 St. George's Terrace, WA 6000 (1300 030 886)

Duty of Disclosure

Before you enter into an insurance contract, you have a duty to tell us anything that you know, or could reasonably be expected to know, may affect our decision to insure you and on what terms.

You have this duty until we agree to insure you.

You have the same duty before you renew, extend, vary or reinstate an insurance contract.

You do not need to tell us anything that:

- reduces the risk we insure you for; or
- is common knowledge; or
- we know or should know as an insurer; or
- we waive your duty to tell us about.

Subject to the Cancellation General Provision, if you do not tell us anything you are required to, we may cancel your contract or reduce the amount we will pay you if you make a claim, or both.

If your failure to tell us is fraudulent, we may refuse to pay a claim and treat the contract as if it never existed.

Claims Made and Notified

Some coverage sections of t*his policy contain claims-made and notified* insuring clauses. This means that those insuring clauses will only cover **Claims** first made against you during the **Policy Period** and notified to the **Insurer** as soon as practicable in the **Policy Period** or any applicable extended reporting period. This Policy may not provide cover for any **Claims** made against you if at any time prior to the commencement of this Policy you became aware of facts which might give rise to those claims being made against you.

Section 40(3) of the *Insurance Contracts Act 1984* provides that where you gave notice in writing to an insurer of facts that might give rise to a claim against you as soon as was reasonably practicable after you became aware of those facts but before insurance cover provided by an insurance contract expires, the insurer is not relieved of liability under the contract in respect of the claim, when made, by reason only that it was made after the expiration of the period of insurance cover provided by the contract.

This Policy excludes prior **Insured Events** (including but not limited to **Claims**) and circumstances as outlined in the "Prior Claims and Circumstances" Exclusion in Section 10 of the Policy Wording.

Privacy Notice

This notice sets out how AIG collects, uses and discloses personal information about:

- **you, if an individual; and**
- **other individuals you provide information about.**

Further information about our Privacy Policy is available at www.aig.com.au or by contacting us at australia.privacy.manager@aig.com or on 1300 030 886.

How We Collect Your Personal Information

AIG usually collects personal information from you or your agents.

AIG may also collect personal information from:

- our agents and service providers;
- other insurers;
- people who are involved in a claim or assist us in investigating or processing claims, including third parties claiming under your policy, witnesses and medical practitioners;
- third parties who may be arranging insurance cover for a group that you are a part of;
- providers of marketing lists and industry databases; and
- publically available sources.

Why We Collect Your Personal Information

AIG collects information necessary to:

- underwrite and administer your insurance cover;
- improve customer service and products and carry out research and analysis, including data analytics; and
- advise you of our and other products and services that may interest you.

You have a legal obligation under the Insurance Contracts Act 1984 to disclose certain information. Failure to disclose information required may result in AIG declining cover, cancelling your insurance cover or reducing the level of cover, or declining claims.

To Whom We Disclose Your Personal Information

In the course of underwriting and administering your policy we may disclose your information to:

- your or our agents, entities to which AIG is related, reinsurers, contractors or third party providers providing services related to the administration of your policy;
- banks and financial institutions for policy payments;
- your or our agents, assessors, third party administrators, emergency providers, retailers, medical providers, travel carriers, in the event of a claim;
- entities to which AIG is related and third party providers for data analytics functions;
- other entities to enable them to offer their products or services to you; and
- government, law enforcement, dispute resolution, statutory or regulatory bodies, or as required by law.

AIG is likely to disclose information to some of these entities located overseas, including in the following countries: United States of America, Canada, Bermuda, United Kingdom, Ireland, Belgium, The Netherlands, Germany, France, Singapore, Malaysia, the Philippines, India, Hong Kong, New Zealand as well as any country in which you have a claim and such other countries as may be notified in our Privacy Policy from time to time.

You may request not to receive direct marketing communications from AIG.

Access to Your Personal Information

Our Privacy Policy contains information about how you may access and seek correction of personal information we hold about you. In summary, you may gain access to your personal information by submitting a written request to AIG.

In some circumstances permitted under the Privacy Act 1988, AIG may not permit access to your personal information. Circumstances where access may be denied include where it would have an unreasonable impact on the privacy of other individuals, or where it would be unlawful.

Complaints

Our Privacy Policy also contains information about how you may complain about a breach of the applicable privacy principles and how we will deal with such a complaint.

Consent

If applicable, your application includes a consent that you and any other individuals you provide information about consent to the collection, use and disclosure of personal information as set out in this notice.

Copyright

Code of Practice

The **Insurer** is a signatory to the General Insurance Code of Practice. This aims to raise the standards of practice and service in the insurance industry, improve the way that claims and complaints are handled and help people better understand how general insurance works. Information brochures on the Code are available upon request.

Dispute Resolution Process

We are committed to handling any complaints about our products or services efficiently and fairly.

If you have a complaint:

(i) contact your insurance intermediary and they may raise it with us;

(ii) if your complaint is not satisfactorily resolved you may request that your matter be reviewed by management by writing to:

The Compliance Manager
AIG Australia Limited
Level 13, 717 Bourke Street
Docklands VIC 3008