QBE Cyber Response Full Proposal Form

1 Applicant details

Registered Company Name:

.....

All other trading names of all entities to be insured:

.....

Registered Company Address:

Postcode .....

Company Website(s) Address(es):

.....

2 Company and financial details

Please indicate the primary and secondary sectors (where appropriate) in which your business operates:

.....

Financial Year End date (FYE): **Date** / /

Currency:

Total revenue including fee income, net profit/loss (before tax), gross wage roll:

Last completed financial year: ☐

Current financial year (est): ☐

Next financial year (est): ☐

Please provide the percentage of gross revenue derived from e-commerce: ☐

Please provide details of any levels of indemnity you have in place from a 3rd party IT service provider, or from any 3rd party accessing, collecting, storing, maintaining, processing, transmitting or otherwise handling your data:

3 Company data

Does your business access, collect, store, maintain, process, transmit, or otherwise handle any of the following?

Type of data	Number of data records	Encrypted at Rest			Encrypted in Transit			Encrypted on mobile devices			% of records in respect of US nationals
Personally identifiable information	☐	Yes ☐	No ☐	N/A ☐	Yes ☐	No ☐	N/A ☐	Yes ☐	No ☐	N/A ☐	☐
Financial account, credit or debit card information	☐	Yes ☐	No ☐	N/A ☐	Yes ☐	No ☐	N/A ☐	Yes ☐	No ☐	N/A ☐	☐
Healthcare or medical information	☐	Yes ☐	No ☐	N/A ☐	Yes ☐	No ☐	N/A ☐	Yes ☐	No ☐	N/A ☐	☐
Government identity information	☐	Yes ☐	No ☐	N/A ☐	Yes ☐	No ☐	N/A ☐	Yes ☐	No ☐	N/A ☐	☐

4 Privacy & Information Security Controls

Please read the following statements and rate your maturity on a scale of 0 (non existent) to 5 (mature) as well as provide further detail of your privacy and information security controls. Indicative characteristics are provided at maturity levels 1, 3 and 5 to guide your self assessment.

4.1 **Governance:** Information security and data privacy are effectively embedded into the organisation's corporate governance and enterprise risk management mechanisms.

Please rate on a scale of 0 (non existent) to 5 (mature)

0

1
> Information security and data privacy priorities, risks and achievements are indirectly reported to senior management, such as Directors/Board.
> Management responsibilities for data privacy and information security are owned and documented.

2

3
> Information security and data privacy priorities, risks and achievements are directly reported to senior management, such as Directors/Board.
> Senior management are accountable for and actively support and promote the importance of information security and data privacy across the business.
> Information security and data privacy risks are identified as part of defined IT or enterprise risk management activities and managed in line with the organisation's risk appetite.

4

5
> The senior individual(s) responsible for information security and data privacy is a member of the senior management team and attends such meetings.
> Senior management play an active role in defining information security and data privacy strategy and priorities.
> There is an assigned member of the board who provides a single point of accountability for privacy and security.

Please provide supporting evidence for your self assessment referencing reporting lines for information security and data privacy and interaction with wider corporate governance.

4.2 **Compliance & Assurance:** The design and effectiveness of the data privacy and information security arrangements across the organisation are independently reviewed and assured on at least an annual basis.

Please rate on a scale of 0 (non existent) to 5 (mature)

0

> There are documented and approved data privacy and information security policies.
> Compliance against the data privacy and information security policies, is monitored by responsible individuals on an ad-hoc basis.

1

2

> Compliance against the information security and data privacy policies and framework are monitored by responsible individuals against defined metrics.
> Business processes control consent and data usage.
> Overall information security and data privacy arrangements are reviewed by an independent internal function (e.g. Internal Audit) or external party on an annual basis.
> Non-compliances and exceptions are formally considered by management and remedial activity taken as required.

3

4

> Industry certifications are in place and attested to by third party bodies (such as PCI-DSS, ISO27001, SOC 2).

5

Please provide supporting evidence for your self assessment referencing your approach to compliance, including any regular audits, and regulatory compliance and industry standards met.

4.3 **Employee Security:** All staff are made aware of their responsibilities in securing your data and the security threats relevant to their role and your organisation.

Please rate on a scale of 0 (non existent) to 5 (mature)

0

> There are documented employee security processes and standards.
> Employees are required to adhere to information security and data privacy policies.
> Some level of ad-hoc training and awareness activities take place.

1

2

> Pre-employment screening is conducted.
> Information security responsibilities, including confidentiality, are included in employment contracts.
> Newly onboarded employees are given induction training, and made aware of relevant policies, processes and standards.
> Annual security refresher training is mandated, including regulatory obligations.
> Return of equipment for leavers and appropriate re-use or disposal.

3

4

> An annual programme of continuous awareness raising and training is in place.
> Regular simulated phishing campaigns are run and direct training.
> Role-based training to provide specific information to key or high-risk staff.
> Effectiveness of awareness activities is monitored and reported (evidence of employee understanding).

5

Please provide supporting evidence for your self assessment referencing your approach to employee security.

4.4 **Data Management:** There is a documented approach to asset identification, data classification & information handling implemented across the business.

Please rate on a scale of 0 (non existent) to 5 (mature)

0

> There is a documented data classification, handling & destruction policy to cover all data processed and handled by the organisation.

1

2

> An inventory of information assets is maintained.
> Staff are trained on data classification and handling.
> Implementation of the policy is user-led.
> Documented business processes for handling data and appropriate authorisations for its use (publishing, sharing, editing).
> Critical data is encrypted at rest (on endpoints and in the cloud), in transit (across the network and email), and on mobile devices (laptops, smartphones etc.).

3

4

> There is technical enforcement, e.g. Data Loss Prevention tools, of the policy.
> All personal, financial, and confidential business data is encrypted at rest (on endpoints and in the cloud), in transit (across the network and email), and on mobile devices (laptops, smartphones etc.).

5

Please provide supporting evidence for your self assessment referencing your critical information assets, and your approach to asset management.

4.5 **Third Party Security:** There are documented and implemented procedures to verify that all third parties who access or otherwise handle your data have the appropriate privacy and security arrangements in place to meet your requirements, and you are protected by appropriate contractual provisions with them.

Please rate on a scale of 0 (non existent) to 5 (mature)

0

> Basic security assessments are performed for a small number of third parties.
> Written agreements are in place with key third parties.

1

2

> A record is maintained of all third-parties who access, store or process information.
> Third parties have completed security self-assessments as part of the procurement process, and standard terms and conditions are in place.
> A third-party risk register is maintained.

3

4

> Independent assurance (SOC2, ISO27001, penetration test etc.) has been obtained about the security arrangements of third parties and specific security contractual clauses are included in agreements.
> Third party security arrangements and compliance are reviewed on an annual basis and during significant changes to scope of services.

5

Please provide supporting evidence for your self assessment referencing any key third party / outsourced relationships you have, and your approach to third party security.

4.6 **Physical & Environment Security:** All premises and IT facilities are physically secured from unauthorised access and protected from environmental hazards.

Please rate on a scale of 0 (non existent) to 5 (mature)

0

> Only staff and authorised visitors have access to premises and IT facilities.
> Visitors sign in and out
> Basic environmental controls, including Uninterruptible Power Supplies (UPS) and air conditioning, are in place in IT facilities.

1

2

> CCTV for entry/exit and common areas.
> Physical access barriers, such as turnstiles, are in place.
> Visitors wear badges to distinguish them.
> Full environmental controls, including raised flooring; fire suppression and backup generators, are in place for IT facilities.

3

4

> Physical access permissions are reviewed on a regular basis.
> Support arrangements are in place to maintain environmental controls, such as a third party contract for maintaining the fire suppression system.
> Visitors are accompanied in restricted areas.
> The same physical and environmental controls are confirmed to be present in outsourced premises and IT facilities.

5

Please provide supporting evidence for your self assessment referencing the numbers of premises and IT facilities, and your approach to physical and environmental security.

4.7 **Incident Management:** There are documented incident response procedures, including full business continuity plans, which are exercised at an operational and management level on at least an annual basis.

Please rate on a scale of 0 (non existent) to 5 (mature)

0

> There is a documented incident response policy.
> There is a documented business continuity plan.

1

2

> There are supporting incident response procedures and plans to reduce the impact of incidents, identify the root cause and communicate incidents to relevant stakeholders.
> All information security incidents are recorded along with lessons learned to prevent re-occurrence.
> Incident response and business continuity plans are exercised at the management level, e.g. table-top exercises,on at least an annual basis.

3

4

> There are supporting security incident response operational playbooks for all incident categories.
> Incident response and business continuity plans are exercised at the operational level, e.g. testing offsite working arrangements, on at least an annual basis.
> There is specialist incident support via dedicated internal resources or specialist third parties.).

5

Please provide supporting evidence for your self assessment referencing your incident response and business continuity plan, and testing procedures.

4.8 **Access Control:** Access to IT resources are controlled through documented procedures and access to privileged resources are protected through authentication.

Please rate on a scale of 0 (non existent) to 5 (mature)

0

> There are documented policies and procedures for access control linked to employee security.
> There is a password policy.
> User accounts are created on the basis of least privilege.

1

2

> Role-based-access-control is applied with clear business justification related to the data to be handled.
> There are no shared or generic accounts; all user accounts use a unique ID.
> Strong passwords are enforced for all IT resources.
> Multi-factor-authentication (MFA) for all administrative accounts and for all remote access.
> Up-to-date records of all privileged user accounts are maintained.

3

4

> There is a privileged account management (PAM) platform in place.
> Access rights reviewed on a quarterly basis, including privileged accounts to confirm they are still required.
> MFA for all users accounts and IT resources.

5

Please provide supporting evidence for your self assessment referencing your access control procedures.

4.9 **Anti Malware Protection:** All endpoints are protected by anti-malware (AM) software that is centrally configured and maintained.

Please rate on a scale of 0 (non existent) to 5 (mature)

0

> Anti-malware tools (including anti-virus software) are deployed to all endpoints.
> Anti-malware tools are kept up-to-date through automated updates.

1

2

> Anti-malware tools are managed via a central console.
> Anti-malware tools are configured to perform on-access and periodic scans.
> Anti-malware tools are configured to detect and remove all known types of malware, e.g. Malware, Rootkits or PUAs (Potentially Unwanted Applications).
> Anti-malware configuration can not be changed by end users (employees).
> USB ports disabled.

3

4

> Endpoint Detection & Response tools/capabilities are deployed to all endpoints.
> Tool configuration and effectiveness are continually reviewed to mitigate emerging threats and reduce false positives.

5

Please provide supporting evidence for your self assessment referencing your anti-malware controls.

4.10 **Email & Internet Security:** All users are protected by email and internet gateway security arrangements (e.g. email and website security filtering).

Please rate on a scale of 0 (non existent) to 5 (mature)

0

1
> Some use of native (inbuilt) protections provided by email service provider and web browsers.
> Laptops are protected by personal firewalls.

2

3
> Email security tools are deployed to provide protection against advanced email-borne malware, phishing and email spoofing.
> Internet security gateway filtering tools are deployed to provide protection against malicious and spoofed websites.

4

5
> Security tool configuration and effectiveness are continually reviewed to mitigate emerging threats and reduce false positives.
> Multiple advanced security tools are deployed to provide multi-layered protection against advanced malware, phishing and malicious websites.

Please provide supporting evidence for your self assessment referencing you're approach to email and internet gateway security.

4.11 **Security Monitoring:** The scope of security monitoring covers all on-premise and cloud environments and your full endpoint estate, and is of sufficient quality to enable effective management of security events and incidents.

Please rate on a scale of 0 (non existent) to 5 (mature)

0

> Logging in place across critical IT systems and services.
> All logs include an accurate date and time stamp.
> Audit logs are maintained for at least 90 days.

1

2

> Logging in place across all systems and services (including IoT and control systems).
> Audit logs record user activities, exceptions, security events, system administrator and system operator activities.
> Monitoring in place to detect unauthorised access, modifications or other malicious behaviour.

3

4

> Monitor of all security events based on policies which allow for alerting of critical events to security administrators.
> Remote monitoring and management services in use and hardened appropriately.
> Logging and monitoring integrated with other security information (Security Information & Event Management - SIEM).

5

Please provide supporting evidence for your self assessment referencing your security monitoring arrangements for all areas of your IT estate.

4.12 **Network Security:** The network is protected by perimeter defences, internal segmentation, and intrusion protection.

Please rate on a scale of 0 (non existent) to 5 (mature)

0

> The network perimeter is protected against unauthorised external connections, such as through the use of firewalls or ACLs (Access Control Lists). **1**

2

> All data in-transit including all authentication data is encrypted across the network.
> There is segmentation between trusted and untrusted, such as between corporate (HQ) and operational (manufacturing) networks.
> Network Access Control (NAC) deployed on critical areas of the network.
> There is some form of intrusion detection system or procedure to detection unauthorised access to the network.
> There is regular review of firewall rules and configuration. **3**

4

> Advanced intrusion detection and prevention systems are implemented at strategic points on the network detection unauthorised access to the network.
> Alerts from intrusion detection and prevention systems are actively monitored and reviewed.
> Network Access Control (NAC) deployed across the whole network and regularly reviewed. **5**

Please provide supporting evidence for your self assessment referencing your network security architecture.

4.13 **Secure IT Configuration & Development:** All IT activities are performed in line with secure configuration and development practices across the IT lifecycle.

Please rate on a scale of 0 (non existent) to 5 (mature)

0

1
> There are documented procedures for maintaining systems and infrastructure.
> Selected servers are built and configured in a standard manner across the IT estate.

2

3
> An inventory of IT assets is maintained.
> IT changes are formally managed and the security impacts are assessed.
> All servers are built and configured in a standard manner across the IT estate.
> The IT estate is centrally managed and controlled, including the ability to remote wipe mobile devices.
> There are secure software development procedures in place across the software lifecycle.
> There is logical separation of development, test and productions environments.

4

5
> Configuration management tools are used to maintain and automate deployment of secure builds.
> Secure software development procedures are applied across all IT activities and reviewed on a regular basis.
> There are procedures for securely managing the end-of-life for hardware and software.

Please provide supporting evidence for your self assessment referencing your approach to secure configuration and development.

4.14 **IT Backup & Disaster Recovery:** There are documented plans to restore critical services and systems following a compromise or loss of availability, which are tested on at least an annual basis.

Please rate on a scale of 0 (non existent) to 5 (mature)

0

1

> There are documented procedures for the backup and recovery of critical systems and services.
> Regular backups are taken of critical systems and data.

2

3

> Retain secured off-site copies of critical software.
> Retain secured off-site backups of critical data.
> Test restores of critical backups regularly.
> Dispose of backup files when no longer required.
> There are documented procedures for the backup and restore of all systems and services.
> There are documented plans for wider IT disaster recovery, including the use of hot recovery sites as required.
> Capacity planning, management (such as load balancing), monitoring performed to ensure adequacy of processing and storage capabilities.

4

5

> Retain secure off-site backups of all data.
> Test restores of all backups regularly.
> Wider IT disaster recovery plans are exercised at least annually.

Please provide supporting evidence for your self assessment referencing your restoration and recovery processes.

4.15 **Technical Vulnerability Management:** All operating systems, databases and applications are under security support from the vendor or distribution, and there is a documented procedure to identify and remediate security vulnerabilities across the IT estate.

Please rate on a scale of 0 (non existent) to 5 (mature)

0

1
> Critical operating systems, databases and applications are under security support from the vendor or distribution (open source).
> There are documented procedures for the identification of security vulnerabilities including the classification of their criticality.

2

3
> All operating systems, databases and applications are under security support from the vendor or distribution.
> Regular vulnerability scanning is performed on critical systems.
> There are documented procedures for the assessment and mitigation of security vulnerabilities (e.g. regular security patching).
> Ad hoc penetration testing.

4

5
> There is a comprehensive programme of regular network and host-based scanning, including web application scanning for OWASP Top 10 vulnerabilities and remediation across the entire estate.
> Regular penetration testing performed across the IT estate.
> IT assets are assessed for risk/business impact to inform the prioritisation of remediation.

Please provide supporting evidence for your self assessment referencing your patching and vulnerability management arrangements.

5 Business Impact

If a business critical cyber-incident were to occur (a hacking event preventing the use of core systems for example), how long would it be before you were to suffer a loss of net profit?

1	2	3	4	5
< 1 hour	1-12 hours	12-24 hours	24-48 hours	48 hours +

How much net profit per day would you expect to lose if such a cyber-incident were to occur?

6 Claims & Circumstances

Have you ever made or reported any claim or any circumstance including against principles/directors that would be covered under this insurance? Yes ☐ No ☐

Have you ever suffered a business outage that has lasted more than 8 hours? Yes ☐ No ☐

If 'Yes', please provide details including date of claim and amounts paid or reserved by insurers and/or details of any business outages suffered:

If 'Yes', what steps have been taken to prevent a reoccurence:

Are there any potential claim(s) or circumstance(s) that are likely to give rise to claim/loss against your company that would fall within the scope of this insurance? Yes ☐ No ☐

If 'Yes', please provide details including estimated cost of claim/loss: Yes ☐ No ☐

6 Claims & Circumstances (Continued)

Have you ever been involved in any dispute or arbitration concerning products, services or intellectual property rights? Yes ☐ No ☐

Have you sustained any loss from the suspected dishonesty or malice of any employee? Yes ☐ No ☐

If 'Yes' to any of the above, please provide details below:

7 Other Information

If you have any other information you deem pertinent please provide it on the final page of this proposal form.

8 Declaration

I/We declare that this proposal has been completed after appropriate enquiry and that the statements and particulars in this proposal (including all attachments, if applicable) are true and that I/We have neither misrepresented or suppressed any material facts.

I/We undertake to inform Underwriters of any material alteration to these facts whether occurring before or after the completion of the contract of insurance.

Signature of Principal/Partner/Director .....

Date / /

9 Additional Information

QBE Insurance
(Singapore) Pte Ltd
Part of QBE Insurance Group Unique Entity No. 198401363C

1 Wallich Street, #35-01 Guoco Tower,
Singapore 078881
Tel: (65) 6224 6633
www.qbe.com/sg