

NOT IF, BUT HOW



Insurance Application Cyber Risk

Please complete the following questionnaire, ensuring accuracy and completeness of all responses and statements. It is important that all relevant information is provided as we rely on the information provided to form the basis of an insurance contract. As such, someone within the company responsible for information security should answer and sign the questionnaire or at least support the person who is answering it by countersigning. If you have no information security resource, then the questionnaire should be completed by a senior representative of your company (owner or board member).

Company Information

Company Name:		Website(s):	
Address:			
Industry:			
Business Description:			

Financial Information

Currency:		Prior Fiscal Year	Current Year	Next Fiscal Year (Forecast)
Revenue:				
Gross Profit:				

Please indicate a percentage split of revenue between the following territories:

United States of America:		%	Europe:		%	International:		%
---------------------------	--	---	---------	--	---	----------------	--	---

Data Governance & Privacy

1. Please identify the nature of sensitive information stored within your organization:

Sensitive Information	No. of Unique Records (Stored)	Sensitive Information	No. of Unique Records (Stored)
☐ Personally Identifiable Info (PII)		☐ Financial Information	
☐ Personal Card Info (PCI)		☐ Social Security Numbers	
☐ Personal Health Info (PHI)		☐ Biometric Information	

2. Please estimate the maximum number of unique records held within a single database:

3. Do you have a Chief Privacy Officer, Data Protection Officer or function equivalent?	☐ Yes ☐ No
4. Do you have a written privacy policy that is reviewed (at least annually) by qualified legal counsel?	☐ Yes ☐ No
5. Do you share any personal data with third parties?	☐ Yes ☐ No

a. If Yes, do you have data sharing agreements in place with all third parties where personal data is shared?	☐ Yes	☐ No
6. Do you obtain authorization prior to sharing customer data with third parties?	☐ Yes	☐ No
7. Do you give data subjects the ability to opt-out of allowing personal data to be shared with third parties?	☐ Yes	☐ No
8. Do you have a process in place to respond to data subject requests (e.g. access requests, right to erasure) and complaints based on applicable data privacy regulations?	☐ Yes	☐ No

A.05 Information Security Policies

1. Do you have a documented corporate-wide policy governing information security?	☐ Yes	☐ No
2. Is your information security policy reviewed (at least annually) and approved by senior management?	☐ Yes	☐ No

A.06 Organization of Information Security

1. The applicant's Information security function is:	☐ Centralized	☐ Decentralized	☐ Hybrid
2. Have you assigned a responsible person for information security (e.g. Chief Information Security Officer)?	☐ Yes	☐ No	
a. If Yes, does this person regularly report to senior level management?	☐ Yes	☐ No	
3. Overall Information Technology Budget (most recent financial year):			
4. Percentage of Information Technology budget allocated to information security (approx.):		%	
5. The following cybersecurity standards, frameworks, or best practices are leveraged by the organization:			
ISO/IEC 27001	☐ N/A	☐ Aligned	☐ Assessed by 3 rd Party
	☐ Certified	Date of Audit:	
NIST CSF 800-53	☐ N/A	☐ Aligned	☐ Assessed by 3 rd Party
	☐ Certified	Date of Audit:	
NERC	☐ N/A	☐ Aligned	☐ Assessed by 3 rd Party
	☐ Certified	Date of Audit:	
Other (provide details):			

Additional commentary:

--

A.07 Human Resource Security

1. Please confirm the total number of employees:	
2. Please confirm the total number of computer users (if different than employee number):	
3. Please confirm the total number of full time IT employees:	
4. Please confirm the total number of full time employees dedicated to information security:	
5. Which of the following information security and privacy trainings are conducted? (Select all that apply)	
☐ Employee training modules	☐ Formal policy acknowledgement
☐ Periodic Bulletins	☐ Awareness Campaigns
6. Percentage of employees that have completed information security training:	%
7. Do you conduct employee phishing campaigns?	☐ Yes ☐ No
a. If Yes, what is the click through failure rate on the latest test?	%
8. How often are phishing campaigns conducted?	
☐ Continuous	☐ Quarterly
☐ Yearly	☐ Other:
9. Do you mandate additional training to those employees who fail to acknowledge phishing emails?	☐ Yes ☐ No

10. Do you have a corporate employee social media policy?	☐ Yes	☐ No
11. Do you perform background checks on employees & contractors who have access to sensitive information?	☐ Yes	☐ No
12. Do you terminate user access rights as part of the employee exit process?	☐ Yes	☐ No

Additional commentary:

A.08 Asset Management

1. Please select the asset types used within the company:

- | | |
|--|---|
| ☐ Endpoints (workstations, laptops, other mobile devices) | ☐ Internal Servers (non-public facing) |
| ☐ External Servers (public internet facing) | ☐ Removable Media Devices |
| ☐ Point of Sale Systems | ☐ Operational Technology (ICS, PLC, SCADA) |
| ☐ ATMs, Payment Terminals, Kiosks | ☐ Networking infrastructure (e.g. firewalls, switches) |
| ☐ Onboard Systems (Aviation, Auto, Fleet, Rail etc.) | ☐ Cloud-hosted servers, regions, buckets |
| ☐ Cloud-hosted applications (e.g. O365) | ☐ Cloud-hosted services (e.g. Cloud VPN, SDN) |

2. In your organisation:

- | | |
|--|--|
| ☐ Hardware is manually inventoried (i.e. spreadsheet) | ☐ Hardware is automatically inventoried (i.e. tool based) |
|--|--|

3. A hardware inventory is updated:	☐ Continuously	☐ Weekly	☐ Monthly	☐ Other:	
-------------------------------------	---------------------------------------	---------------------------------	----------------------------------	---------------------------------	--

4. What percentage of your hardware is inventoried?

- | | | | |
|--|--|--|--|
| ☐ Less than 25% | ☐ Between 25% and 50% | ☐ Between 50% and 75% | ☐ More than 75% |
|--|--|--|--|

5. Software inventory is updated:	☐ Continuously	☐ Weekly	☐ Monthly	☐ Other:	
-----------------------------------	---------------------------------------	---------------------------------	----------------------------------	---------------------------------	--

6. What percentage of your software is inventoried

- | | | | |
|--|--|--|--|
| ☐ Less than 25% | ☐ Between 25% and 50% | ☐ Between 50% and 75% | ☐ More than 75% |
|--|--|--|--|

7. If you inventory hardware and/or software assets, do you have an asset classification policy that is enforced?	☐ Yes	☐ No
---	------------------------------	-----------------------------

8. Are all mobile devices managed using a Mobile Device Management (MDM) solution?	☐ Yes	☐ No
--	------------------------------	-----------------------------

9. Do you disable media ports or restrict usage to only encrypted removable storage devices?	☐ Yes	☐ No
--	------------------------------	-----------------------------

10. Do you allow employees to use personal mobile devices to access company data (e.g. email)?	☐ Yes	☐ No
--	------------------------------	-----------------------------

a. If Yes, do you have a Bring Your Own Device (BYOD) policy in place that governs usage and controls?	☐ Yes	☐ No
--	------------------------------	-----------------------------

11. Is a Web Application Firewall (WAF) used to protect publicly exposed web application?	☐ Yes	☐ No
---	------------------------------	-----------------------------

12. Do you ensure that all publicly facing ports are protected by a pre-configured firewall that blocks unauthorised network traffic?	☐ Yes	☐ No
---	------------------------------	-----------------------------

13. Do you regularly scan publicly accessible ports and ensure unnecessary ones are locked down?	☐ Yes	☐ No
--	------------------------------	-----------------------------

Additional commentary:

A.09 Access Control

1. Do you restrict user access (employees, contractors etc.) on a business need-to-know & least-privilege basis?	☐ Yes	☐ No
--	------------------------------	-----------------------------

2. Do you have a central Identity & Access Management ("IAM") system for assigning and revoking access rights?	☐ Yes	☐ No
--	------------------------------	-----------------------------

3. Do you have a formal process in place for assigning and revoking user accounts and access rights?	☐ Yes	☐ No
--	------------------------------	-----------------------------

4. Do assets owners review access rights at least annually?	☐ Yes ☐ No
5. Do you enforce multifactor authentication (MFA) for access to the following: <i>(Select all that apply)</i>	
☐ Critical & Sensitive Information	☐ Admin & Privileged Accounts
☐ Remote Connections	☐ Portable Devices
☐ Independent contractor & vendors	
6. Do you allow Remote Desktop Protocol (RDP) connections? ☐ Yes ☐ No	
a. If Yes, do you implement any of the following controls on RDP connections: <i>(Select all that apply)</i>	
☐ VPN access only	☐ MFA for access
☐ Network level authentication	☐ RDP honeypots(s)
7. Please confirm the type(s) of multifactor authentication in place: <i>(Select all that apply)</i>	
☐ Push notification	☐ Authenticator app
☐ SMS message	☐ Device certificate
☐ Biometric	☐ Token/physical key
☐ Secondary email	☐ Other:
8. Do you manage privileged accounts through an access management tool (e.g. <i>CyberArk, Delinea, BeyondTrust</i>)? ☐ Yes ☐ No	
a. If Yes, which of the following accounts are enrolled into the PAM tool? <i>(Select all that apply)</i>	
☐ Privileged User Accounts	☐ Domain Admin Accounts
☐ Local Admin Accounts	☐ Application Accounts
☐ Domain Service Accounts	☐ Backup Accounts
☐ Service Accounts	☐ Linux Accounts
9. Which of the following features are enabled on the PAM tool? <i>(Select all that apply)</i>	
☐ Credential Rotation	☐ Credential Vaulting
☐ Credential Time-out	☐ MFA
☐ Real time monitoring of activity	☐ One-time Passwords
10. Is logging and alerting configured for all privileged account activity? ☐ Yes ☐ No	
11. Are domain admin accounts limited to administrative functions only? <i>(e.g. no email/internet access)</i> ☐ Yes ☐ No	
12. Please provide the number of service accounts in the domain admin group? 	
13. Do you configure service accounts using the principle of least privilege? ☐ Yes ☐ No	
14. Do you configure service accounts to deny interactive log-ins? ☐ Yes ☐ No	
15. Do you log the activity of service accounts that are able to override system or application controls (e.g. elevation of privileges, lateral movement etc.)? ☐ Yes ☐ No	
16. Do you prohibit local admin rights on workstations for users? ☐ Yes ☐ No ☐ Sometimes	

Additional commentary:

A.10 Cryptography

1. Do you enforce the use of encryption over all external communication lines (e.g. website, email, wireless)?	☐ Yes ☐ No
2. Do you enforce the use of encryption of sensitive information while at rest (e.g. on premise, mobile device, cloud)?	☐ Yes ☐ No

Additional commentary:

A.11 Physical & Environmental Security

1. Please enter how many offices/locations you currently maintain:	
2. Please enter any offices/locations that have data rooms/closets:	
3. Do you implements any of the following security controls for data rooms/closets in your offices: <i>(Select all that apply)</i>	

- | | | |
|---|--|---|
| ☐ Access is controlled by locked doors | ☐ Cameras are used to monitor access | ☐ Remote monitoring is in place 24/7 |
| ☐ Access is limited to IT personnel | ☐ Uninterruptible Power Source in place | ☐ Onsite monitoring is in place 24/7 |
| ☐ Biometrics are used for access control | | |

4. Please enter the number of data centres owned and operated by your organization:

Do you implement any of the following security controls for data centres that you own or operate: *(Select all that apply)*

- | | | |
|---|--|---|
| ☐ Access is controlled by locked doors | ☐ Cameras are used to monitor access | ☐ Remote monitoring is in place 24/7 |
| ☐ Access is limited to IT personnel | ☐ Uninterruptible Power Source in place | ☐ Onsite monitoring is in place 24/7 |
| ☐ Biometrics are used for access control | | |

5. Does your company operate a clean desk policy at all sites?

☐ Yes ☐ No

Additional commentary:

A.12 Operations Security

1. What type of endpoint protection solution is used? *(Select all that apply)*

- ☐ Signature based antivirus ☐ Behavioural based antivirus ☐ Advanced EDR ☐ None ☐ Other

2. Please select the vendor(s) used within your organisation:

- | | | | | | | |
|---|---|--------------------------------------|------------------------------------|---------------------------------|----------------------------------|-----------------------------------|
| ☐ Microsoft Defender | ☐ CrowdStrike Falcon | ☐ SentinelOne | ☐ F-Secure | ☐ Cisco | ☐ Cylance | ☐ Symantec |
| ☐ Carbon Black Cloud | ☐ Check Point | ☐ McAfee | ☐ Palo Alto | ☐ Sophos | ☐ Other: | |

3. What is the deployment percentage on the following endpoints?

Workstations: % Servers: % Laptops: %

4. Please state the number of malware blocked by host based anti-malware within the past 12 months:

5. Do you take backups of any of the following: *(Select all that apply)*

- | | | | | | | |
|---------------------|-----------------------------------|--------------------------------|---------------------------------|----------------------------------|---------------------------------|--|
| Critical Data: | ☐ Mirrored | ☐ Daily | ☐ Weekly | ☐ Monthly | ☐ Other: | |
| Servers: | ☐ Mirrored | ☐ Daily | ☐ Weekly | ☐ Monthly | ☐ Other: | |
| Domain Controllers: | ☐ Mirrored | ☐ Daily | ☐ Weekly | ☐ Monthly | ☐ Other: | |
| Workstations: | ☐ Mirrored | ☐ Daily | ☐ Weekly | ☐ Monthly | ☐ Other: | |

6. How are your backups stored? *(Select all that apply)*

- | | | | | | |
|----------------|--------------------------------------|---|---|--------------------------------|------------------------------------|
| Critical Data: | ☐ On Premises | ☐ Offsite/External | ☐ Physical/Offline | ☐ Cloud | ☐ Encrypted |
| Servers: | ☐ On Premises | ☐ Offsite/External | ☐ Physical/Offline | ☐ Cloud | ☐ Encrypted |
| Workstations: | ☐ On Premises | ☐ Offsite/External | ☐ Physical/Offline | ☐ Cloud | ☐ Encrypted |

7. If cloud backups are used, is this a syncing service (e.g. DropBox, OneDrive, SharePoint, Google Drive etc.)

☐ Yes ☐ No

8. Are unique backup credentials stored separately from other user credentials?

☐ Yes ☐ No

9. Are backup processes tested to ensure data can be restored with minimal impact to the business?

☐ Yes ☐ No

10. Do you log activities for business critical services & applications (e.g. logins, privilege escalation etc.)

☐ Yes ☐ No

11. Are your audit logs immutable?

☐ Yes ☐ No

12. What is the average time to patch for the following systems: *(Select most relevant)*

- | | | | | | | | |
|------------------------|------------------------------------|----------------------------------|-----------------------------------|------------------------------------|------------------------------------|---------------------------------|--|
| Workstations: | ☐ Automatic | ☐ < 1 day | ☐ < 7 days | ☐ < 30 days | ☐ > 30 days | ☐ Other: | |
| Critical Applications: | ☐ Automatic | ☐ < 1 day | ☐ < 7 days | ☐ < 30 days | ☐ > 30 days | ☐ Other: | |

Internal Servers:	☐ Automatic	☐ < 1 day	☐ < 7 days	☐ < 30 days	☐ > 30 days	☐ Other:	
Perimeter Systems:	☐ Automatic	☐ < 1 day	☐ < 7 days	☐ < 30 days	☐ > 30 days	☐ Other:	

13. Do you install critical security patches (CVSS > 9.0) on internet-facing IT systems and applications:

☐ Within 24 hours ☐ Within 7 days ☐ Within 1 month ☐ More than 1 month

14. Do you regularly conduct vulnerability scanning across your internal and external-facing assets? ☐ Yes ☐ No

15. Please estimate the percentage of your network that is covered by the scans: %

16. Patch levels are monitored and tracked using: ☐ Automatic Scanning ☐ Manual process ☐ Not tracked

17. Do you technically prohibit users from installing unauthorised software on their devices? ☐ Yes ☐ No

18. Do you have a whitelist of software that users and system administrators are permitted to install? ☐ Yes ☐ No

19. Do you rely on systems, software, or hardware that is considered “end-of-life” (EOL) by the manufacturers. ☐ Yes ☐ No

a. If Yes, does your company implement any of the following? *(Select all that apply)*

- ☐ Segregation from wider network and internet ☐ Extended support purchased (when available)
☐ Additional monitoring

Additional commentary:

--

A.13 Communications Security

1. How is your email hosted: ☐ Cloud ☐ On premises

2. Is web-based email available to employees? ☐ Yes ☐ No

3. Are logins to web-based email monitored with alerts for suspicious activity implemented? ☐ N/A ☐ Yes ☐ No

4. Is multi-factor authentication (MFA) in place for web-based email logins? ☐ N/A ☐ Yes ☐ No

5. What type of email filtering is deployed? *(Select all that apply)*

- ☐ Gateway based (e.g. Mimecast/Proofpoint) ☐ Machine learning/Behaviour based ☐ Supported by User Reporting
☐ Provider based (e.g. Office 365/Gmail) ☐ None

6. Do you implement any of the following controls to protect against malicious emails? ☐ DKIM ☐ SPF ☐ DMARC

7. Do you utilize a Data Loss Prevention (DLP) product for email? ☐ Yes ☐ No

8. Is a DLP solution in use on endpoints, external and internal (including email) servers? ☐ Yes ☐ No

a. If Yes, is the DLP solution configured in: ☐ Audit mode ☐ Block mode ☐ Block with override mode

9. Do you scan incoming emails for malicious attachments and/or links? ☐ Yes ☐ No

10. Do you have the ability to automatically quarantine, detonate and evaluate attachments? ☐ Yes ☐ No

11. Are blocked emails classed as incidents and remediated? ☐ Yes ☐ No

12. Please state the number of malicious emails blocked over the past 12 months:

13. Do you tag external emails to alert employees that the message originated from outside the organization? ☐ Yes ☐ No

14. How is web traffic filtered? ☐ Host/DNS based ☐ Network based ☐ None

15. Do you protect your web-servers against "DDoS" attacks (e.g. utilising a content delivery network provider)? ☐ Yes ☐ No

16. Are IP addresses connecting to your non-internet facing servers whitelisted? ☐ Yes ☐ No

17. Do you blacklist IP addresses on your internet facing servers?	☐ Yes	☐ No
18. Do you have the capability to block suspicious requests from your network environment?	☐ Yes	☐ No
19. Number of suspicious requests detected within the past 12 months:		
20. Have you configured host-based and network firewalls to disallow inbound connections by default?	☐ Yes	☐ No
21. What percentage of systems have a firewall access control list (inbound & outbound rules) configured?		%
22. Do you perform periodic reviews of firewall rules to ensure configurations are on a need-to-have basis?	☐ Yes	☐ No
23. Do you utilize any of the following technologies to physically or logically segregate your network?		
☐ Air Gap ☐ DMZ ☐ Firewall ☐ VLAN		
a. If VLAN is selected, describe the degree to which traffic is restricted & the technical control is used to enforce segmentation:		

Do you segment your network based on any of the following: *(Select all that apply)*

- | | | |
|---|--|---|
| ☐ Business Unit | ☐ Asset criticality | ☐ Classification of data stored |
| ☐ Geography/Region | ☐ Asset functionality | ☐ Classification of data processed |

Additional commentary:

A.14 System Acquisition, Development & Maintenance

1. Do you implement a hardened baseline configuration materially rolled out across servers and workstations?	☐ Yes	☐ No
2. Do you have a secure coding baseline in place (e.g. peer reviews & maintenance requirements)?	☐ N/A	☐ Yes ☐ No
3. Are your developers regularly trained in secure programming techniques and code reviews?	☐ N/A	☐ Yes ☐ No
4. Do you conduct security tests or code analysis during system development, before go-live and after system changes take place?	☐ N/A	☐ Yes ☐ No
5. Does confidential test data require the same security controls as confidential data on production systems?	☐ Yes	☐ No
6. Do you ensure that any acquired applications/functions and code is free from known vulnerabilities?	☐ Yes	☐ No

Additional commentary:

A.15 Supplier Relationships

1. Do you identify & categorise third party vendors based on their access to company systems and/or data?	☐ Yes	☐ No
2. Is an information security assessment performed on vendors at due diligence stage with findings addressed?	☐ Yes	☐ No
3. Do you perform periodic audits of vendors and enforce the right to audit in contractual agreement?	☐ Yes	☐ No
4. Do vendor agreements require levels of security commensurate with your own information security standards?	☐ Yes	☐ No
5. Do you periodically review and update vendor access rights?	☐ Yes	☐ No
6. Do you restrict vendor access to limited time-windows and monitor their access to your network?	☐ Yes	☐ No

Additional commentary:

A.16 Incident Management

1. Do you have an information security incident response plan?		☐ Yes	☐ No
a. If Yes, the incident response plan: <i>(Select all that apply)</i>			
☐ Is exercised (at least annually)	☐ Assigns roles to stakeholders	☐ Addresses preservation of forensic evidence	
☐ Defines incident criticality levels	☐ Has playbooks for specific incidents (e.g. ransomware)		
2. Do you have an incident response or digital forensic outsourcing retainer agreement in place?		☐ Yes	☐ No
a. If Yes, please provide details of the vendor:		Vendor:	
3. Are you utilising a Security Incident Event Management (SIEM) solution?		☐ Yes	☐ No
		Vendor:	
4. How are security incident alerts monitored and responded to?			
☐ Internal SOC	☐ External SOC/MSSP	☐ Not actively monitored	☐ Other:
5. Is the full scope of the SOC operating on a 24/7/365 basis?		☐ Yes	☐ No
6. Does your 24/7/365 service have the authority to contain/isolate systems following a suspicious event?		☐ Yes	☐ No
7. Please state the percentage of assets monitored real time:			%
8. Please state the number of intrusion and/or exfiltration attempts over the past 12 months:			
9. Please state the number of escalated security events in the past 12 months:			
10. Please state the maximum number of devices affected by the most significant security event in the past year:			
11. Please state the mean time for your organisation to detect a security event:			hrs
12. Please state the mean time for your organisation to remediate affected devices:			hrs

Additional commentary:

A.17 Business Continuity Management

1. Do you have a written business continuity or disaster recovery plan that addresses network outages & cyber-attacks?		☐ Yes	☐ No
a. If Yes, is this tested annually with critical deficiencies remediated?		☐ Yes	☐ No
2. What is your Recovery Time Objective (RTO) for critical systems?			
☐ Less than 6 hrs	☐ Between 6 and 12hrs	☐ Between 12 and 24hrs	☐ Between 24 and 48hrs
☐ More than 48hrs			
3. Do you have a defined Recovery Point Objective (RPO) for critical systems?		☐ Yes	☐ No
4. Have you planned for redundancy for your critical system infrastructure?		☐ Yes	☐ No
a. If Yes <i>(Select all that apply)</i> :		☐ Hot Site	☐ Real-time cloud replication
		☐ Fall back cloud infrastructure	☐ Cold Site
5. Do you conduct redundancy testing at least annually to ensure that failover works as intended?		☐ Yes	☐ No

Additional commentary:

Multimedia Assessment *(If coverage is required)*

1. Do you have a process in place to review media content (e.g. website, social media) for any of the following: <i>(Select all that apply)</i>			
☐ Copyright Infringement	☐ Trademark Infringement	☐ Invasion of Privacy	☐ Libel or Slander

2. Do you require reviews to be conducted under the supervision of qualified legal counsel? ☐ Yes ☐ No

3. Do you have a procedure for responding to any of the above infringing content (e.g. notice and take-down) ☐ Yes ☐ No

4. With respect to your website(s), does your company:

☐ Record visitor acceptance of terms of use before granting access ☐ Allow third party content (including music & video)

5. For any third party content, do you have procedures in place to secure rights for using such content? ☐ Yes ☐ No

6. Do you allow third parties to post content directly on to your website(s)? ☐ Yes ☐ No

7. Do you retain the right to remove any such third party content that violates your acceptable terms of use? ☐ Yes ☐ No

Additional commentary:

Payment Card Information Assessment *(If applicable)*

1. Do you accept card payments for goods and/or services? ☐ Yes ☐ No

2. How many transactions do you process each year?

☐ Level 1 (greater than 6m) ☐ Level 2 (between 1m & 6m) ☐ Level 3 (between 20k and 1m) ☐ Level 4 (less than 20k)

3. How do you process payment card transactions? *(Select all that apply)*

☐ Strictly card-not-present (e-commerce, mail/telephone) ☐ Standalone terminals ☐ Web based virtual terminals

☐ Payment applications connected to a computer network (incl. via embedded applications within point of sales system)

☐ Other *(please describe)*:

4. Do you store payment card data on your network? ☐ Yes ☐ No

a. If Yes, is payment card data either encrypted or tokenised at all times? ☐ N/A ☐ Yes ☐ No

5. Do you comply with the relevant Payment Card Industry Data Security Standard? ☐ Yes ☐ No

a. If No, please describe the current status of compliance work:

6. Do you transact all payments through a payment processor? ☐ Yes ☐ No

a. If Yes, please provide the vendor(s) used:

7. Has the payment processor provided you with evidence of its PCI DSS compliance? ☐ Yes ☐ No

Additional commentary:

Biometric Information Assessment *(If applicable)*

1. Do you collect, receive or store any of the following biometric data on individuals: *(Select all that apply)*

☐ Fingerprint ☐ Voiceprint ☐ Retina/Iris scan ☐ Hand scan ☐ Face Geometry ☐ Other:

2. Do you clearly outline to individuals how any biometric information will be collected, used and/or destroyed? ☐ Yes ☐ No

3. Do you obtain written consent from individuals prior to collection, receipt or retention of biometric information? ☒ Yes ☐ No

4. Do you have a retention schedule outlining how long biometric information is retained? ☐ Yes ☐ No

5. Do you sell, lease, trade or otherwise profit from the biometric information of individuals? ☐ Yes ☐ No

6. Do you subject biometric data to any of the following measures? *(Select all that apply)*

☐ Encryption at rest ☐ Encryption in transit ☐ Additional access controls ☐ Segregated storage

Additional commentary:

Claims & Insurance History

Do you hold or have you held insurance providing the same or similar coverage as the insurance being applied for? ☐ Yes ☐ No

Has any insurer cancelled or non-renewed a policy that provided the same or similar coverage as the insurance being applied for? ☐ Yes ☐ No

In the last five years has the applicant received or sustained, or are there currently pending, any claims, complaints or incidents which may be covered under the proposed insurance? ☐ Yes ☒ No

Do you have knowledge of any fact, circumstance, situation, event or transaction which may give rise to a claim or loss under the proposed insurance? ☐ Yes ☐ No

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

Signed:

Title:

Print Name:

Date: