Cyber & Technology Risk Application

U.S. New Policy Placement

**Click the section names to jump
to the page where it starts**

I. General information

PLEASE COMPLETE EACH SECTION.

Name & address of firm

Full name:

Address:

City: State: ZIP/postcode:

Website:

Individual completing application form information

Full name:

Surname:

Email:

Applicant's principal contact in the event of a security or privacy breach

Name: Email:

Title: Phone:

Type of business

Sole proprietor   Corporation   Partnership   Other

Date established:

Business description:

ANNUAL REVENUES

Healthcare applicants: Please provide net patient services revenues. All other applicants — please provide gross revenues.

	Last complete financial year	Current year (estimate)	Next year (estimate)
U.S. revenue	USD	USD	USD
International revenue	USD	USD	USD
Gross profits	USD	USD	USD

Do you generate revenues and have a presence i.e. "an establishment" in territories outside the U.S.?	Yes	No	N/A

If 'Yes', please provide a breakdown by appendix to this application. Please note that revenues in Canada and Australia should be further broken down by province and state for tax purposes.

Do you generate revenues and have a presence, i.e., "an establishment", in territories Inside the EEA (excluding U.K.)?	Yes	No	N/A

If 'Yes', please list the territories:

Approximate share of revenue attributable to:

Last complete financial year	**% online trading**
	% business to business
	% business to consumer

Changes to the business:

Does the Applicant anticipate any changes in business activities, mergers, acquisitions, or operations during the next 12 months? If 'Yes', please describe in an appendix to this application.	Yes	No	N/A

Please describe any acquisitions, divestitures, and changes to business operations over the past 12 months.

Are newly acquired companies required to meet certain cybersecurity standards before they are connected to the network?	Yes	No	N/A
Is a cybersecurity audit part of the formal acquisition process?	Yes	No	N/A

II. Risk assessment

CYBERSECURITY GENERAL INFORMATION

Throughout this application, there are several important terms. For clarity, please use the following definitions to guide your answers.

- **Vital Assets:** Assets which are key to the organization's success and operation. **Vital assets** include, but are not limited to, applications which support business production, applications which store business critical and/or sensitive data, and core technology services such as directory services, document repositories, and email.
- **Domain Administrator:** User accounts, excluding **Service Accounts**, which are **privileged** (see below). In an Active Directory environment, this would include Enterprise Admins, Domain Admins, and the (built-in domain) Administrators groups, including nested groups/accounts. In Azure, this would include Global Administrators, Hybrid Identity Administrators, and **Privileged** Role Administrators.
- **Service Accounts:** Accounts used for running applications and other processes. They are not typically used by humans.
- **Privileged:** Any account having administrative rights in whatever solution is in use for directory services, identity provider (IdP), rights management, etc. In an Active Directory environment, this would include Enterprise Admins, Domain Admins, and the (built-in domain) Administrators groups, including nested groups/accounts. In Azure, this would include Global Administrators, Hybrid Identity Administrators, and **Privileged** Role Administrators.

1. Annual IT budget: $

2. Percentage of IT budget spent on cyber security: %

3. Full-time IT employees:

4. Full-time cybersecurity employees:

5. How centralized is the Applicant's information security program? (Choose one)

     a. Information security at the Applicant is centrally managed, and the policies apply to all operations. Where exceptions are made, it's by asset only (as opposed to by operation/legal entity).

     b. Information security at the Applicant is centrally managed, but exceptions are made for certain operation/legal entities. The controls as outlined below apply to greater than or equal to 98% of total endpoints.

     c. Information security at the Applicant is centrally managed, but exceptions are made for certain operation/legal entities. The controls as outlined below apply to less than 98% of total endpoints.

     d. Information security at the Applicant is federated, but the controls outlined below apply to greater than or equal to 98% of total endpoints.

     e. Information security at the Applicant is federated, and the controls outlined below apply to greater than 50% of total endpoints, but less than 98% of total endpoints.

     f. Information security is managed by individual legal entities or operating units. The controls below are based on a survey of all entities and operating units.

     g. Don't know/other — Add addendum if other.

6. Does the Applicant:

a. Have a Data Protection Officer or someone in charge of data security?	Yes	No	N/A
b. Administer a corporate-wide policy governing security, privacy, and acceptable use of company property for all employees and independent contractors?	Yes	No	N/A
i. If 'Yes', does acceptable use policy include consequences for policy violations?	Yes	No	N/A
ii. Are users disallowed from accessing social media platforms from organizational assets except where there is a defined business need?	Yes	No	N/A
iii. Are users disallowed from accessing personal email from organizational assets?	Yes	No	N/A
iv. Are administrators explicitly disallowed from internet use and personal email from their **privileged** accounts?	Yes	No	N/A
v. Are users and administrators responsible for keeping their computers and accounts safe from common risks or issues?	Yes	No	N/A
vi. Are users and administrator required to report suspected violations?	Yes	No	N/A
c. Perform background checks on all employees and independent contractors with access to sensitive data?	Yes	No	N/A
d. Restrict user access to sensitive data/information based upon the job function of the employee or independent contractor?	Yes	No	N/A
i. If 'Yes', is such access reconsidered on at least an annual basis?	Yes	No	N/A
7. Does the Applicant use a third party or Managed Service Provider to administer their technology?	Yes	No	N/A

a. If 'Yes', select all that are true: Applicant utilizes an MSP for:

Vital assets	Security operations	Data backup and recovery
Cloud transformation	Software development	Other (please describe)

b. If 'Yes', is the third party or Managed Service Provider given persistent access to the Applicant's resources, not needing authorization to connect?	Yes	No	N/A
8. Does the Applicant have an inventory of all data stores, which includes the data owners, the asset it is stored on, sensitivity, retention limits and disposal requirements for at least all sensitive data?	Yes	No	N/A
a. If 'Yes', is it updated at least annually?	Yes	No	N/A
9. Has the Applicant defined and documented all **vital assets**?	Yes	No	N/A
a. If 'Yes', is the vital asset inventory updated at least quarterly?	Yes	No	N/A
10. Does the Applicant have a process to actively identify **vital assets**?	Yes	No	N/A
11. Does the Applicant prioritize **vital assets** by importance to business operations?	Yes	No	N/A
12. Does the Applicant have an inventory of all hardware assets, including end user devices, network devices, appliances, IoT devices, and servers?	Yes	No	N/A
a. If 'Yes', does it contain:	Yes	No	N/A

Static IP address   Hardware address   Machine name   Asset owner

b. What frequency is the inventory updated?

Annually   Semi-annually   Quarterly   Other

13. Does the Applicant have a process to discover hardware assets on its network?	Yes	No	N/A
a. If 'Yes', how frequently is process run?	Yes	No	N/A

Continuously   Daily   Weekly   Monthly   Other

14. Does the Applicant have an inventory of all licensed software? Yes No N/A

    a. If 'Yes', what frequency is the inventory updated?

        Annually   Semi-annually   Quarterly   Other

15. Does the Applicant have a process to decommission unused systems? Yes No N/A

16. Does the Applicant use on-premises Microsoft Active Directory, regardless of whether it is authoritative? Yes No N/A

17. Please state the number of servers operated by or on behalf of the Applicant:

18. Please state the number of endpoints operated by or on behalf of the Applicant:

Desktops: Laptops: Other (please specify):

19. Please state the percent of critical systems hosted:

    On premises   %   In a cloud environment   %

If the Applicant has any further comments on questions in the section above, please elaborate below:

DATA ASSESSMENT

1. Please identify nature of sensitive information stored by the Applicant:

Sensitive information	Yes	No	N/A	Records held (estimated)
a. Personally identifiable information				
b. Medical records				
c. Financial information				
d. Driver license numbers				
e. Social Security/National Insurance numbers				
f. Other (please specify below)				

2. Please estimate the total number of unique individuals for whom records are currently stored by the Applicant.

3. In respect of 2., to the right, please estimate the maximum number of records held within a single database:

4. Does the Applicant process data for third-party companies? Yes No N/A

    If 'Yes', please estimate the total number of records processed:

If the Applicant has any further comments on questions in the section above, please elaborate below:

EMPLOYEES

Does the Applicant:

1. Require users to change passwords on at least a quarterly basis?	Yes	No	N/A
2. Require strong passwords for administrator rights, e.g., 10 characters using a mix of alphabetic, numeric, and other characters?	Yes	No	N/A
3. Have a solution to prevent users from setting common and known-compromised passwords, even if they meet complexity requirements? (e.g. "1g2w3e4r5t" and "Passw0rd!")	Yes	No	N/A
4. Enforce rotation of administrator access credentials at least every 30 days?	Yes	No	N/A
5. Require all employees and independent contractors to undergo annual cybersecurity training including phishing?	Yes	No	N/A
6. Terminate user access rights as part of its employee and independent contractor exit processes?	Yes	No	N/A

7. Please confirm the total number of employees.

8. Please confirm the total number of computer users, if different than employee count.

If the Applicant has any further comments on questions in the section above, please elaborate below:

MULTIFACTOR AUTHENTICATION

Does the Applicant:

1. Require multifactor authentication for the following access?	Yes	No	N/A
a. Critical information inside the network	Yes	No	N/A
b. Remote network access	Yes	No	N/A
i. VPN	Yes	No	N/A
ii. VDI	Yes	No	N/A
iii. Sensitive cloud applications	Yes	No	N/A
iv. Sensitive web applications	Yes	No	N/A
c. Administrator and **privileged** accounts	Yes	No	N/A
d. Personal devices when connecting with the network	Yes	No	N/A
e. Independent contractors and vendors accessing the network	Yes	No	N/A
f. Independent contractors and vendors accessing sensitive cloud or web applications	Yes	No	N/A
2. Allow External Remote Desktop Protocol (RDP)? If 'Yes', are the following implemented:	Yes	No	N/A
a. VPN access only	Yes	No	N/A
b. Multifactor authentication for access	Yes	No	N/A
c. Network level authentication enabled	Yes	No	N/A
d. RDP honeypot(s)	Yes	No	N/A
e. Other (Please identify)	Yes	No	N/A

3. Confirm the type(s) of MFA in place:

Push notification	SMS/test message	Biometric
Authenticator app	Secondary email	Certificate based
Token/physical security key	Other	

If the Applicant has any further comments on questions in the section above, please elaborate below:

PRIVILEGED ACCESS MANAGEMENT

Does the Applicant:

1. Manage **privileged** accounts using tooling (e.g., CyberArk, PAM)?	Yes	No	N/A
2. Enroll any of the following accounts into a PAM tool?	Yes	No	N/A

Privileged user accounts	**Service accounts**
Domain administrative accounts	Local administrative accounts
Domain **service accounts**	Application accounts
Backup accounts (used to manage or access backups)	Linux accounts

Other:

If 'No', please provide additional information for any local administrative accounts that are not enrolled into the PAM tool:

a. Please confirm that identical local admin credentials are not used (i.e., there is not a common username and password used for each local admin accounts).	Yes	No	N/A

b. Please provide details below on how unauthorized local admin privilege escalation on workstation is detected:

c. Have you implemented Microsoft's Local Administrator Password Solution (LAPS)?	Yes	No	N/A

3. Enabled the following features on the PAM tool:

a. Please confirm that identical local admin credentials are not used (i.e., there is not a common username and password used for each local admin accounts)	Yes	No	N/A
b. Credential time-out (please state time after which account locks):	Yes	No	N/A
c. One-time passwords	Yes	No	N/A
d. Credential rotation	Yes	No	N/A
e. MFA	Yes	No	N/A
f. Real-time monitoring of account activity/detection of suspicious activity	Yes	No	N/A

4. How often are all **privileged** accounts (such as those used in Active Directory and SaaS solutions as well as Service and Local accounts) inventoried and reviewed? (If less than annually or not inventoried and refreshed, please provide explanation).

5. Is logging and alerting configured for **privileged** account usage/changes?	Yes	No	N/A
6. Are **domain administrator** accounts unique, separate accounts from other accounts used for everyday activities?	Yes	No	N/A

7. Can **Domain Administrator** accounts can only be used from **Privileged** Access Workstations (which do not have access to internet or email?	Yes	No	N/A
8. Is there a log of all actions by **Domain Administrator** accounts for at least the past thirty days?	Yes	No	N/A

9. Please provide a count of the **Domain Administrator** accounts.

LOCAL ADMINISTRATIVE & SERVICE ACCOUNTS

Does the Applicant:

1. Prohibit workstations from local admin rights:

a. All of the time?	Yes	No	N/A
b. Case by case?	Yes	No	N/A
2. Have an inventory of all **privileged service accounts**?	Yes	No	N/A

If 'Yes', how frequently is it reviewed and updated?

Annually   Semi-annually   Quarterly   Other

3. Please provide number of **privileged service accounts**:

a. For each **privileged** service account included above, please use the table provided in Supplement C of application.

4. Configure **service accounts** using the principle of least privilege?	Yes	No	N/A
a. Are **service accounts** tiered such that different accounts are used to interact with workstations, servers, and authentication servers, even for the same service?	Yes	No	N/A
5. Configure **service accounts** to deny any interactive logon?	Yes	No	N/A

If 'Yes', please confirm the percentage: %

6. Have specific monitoring rules in place for **service accounts** to alert for any abnormal behavior?	Yes	No	N/A
7. Require service account passwords to be ≥ 25 characters?	Yes	No	N/A
8. Require service account passwords to be rotated on a regular basis?	Yes	No	N/A

If 'Yes', how frequently?

Annually   Semi-annually   Quarterly   Other

If the Applicant has any further comments on questions in the section above, please elaborate below:

NETWORK OVERVIEW

Does the Applicant:

1. Intrusion Detection Solution (IDS)? Product name:	Yes	No	N/A
2. Intrusion Detection Solution (IDS)? Product name:	Yes	No	N/A

	Yes	No	N/A
3. Endpoint Protection Platform (EPP)? Product name:	Yes	No	N/A
a. Does this include: Endpoints/workstations Servers			
b. Do capabilities include isolation and containment?	Yes	No	N/A
c. Do capabilities include behavioral detection and exploit mitigation?	Yes	No	N/A
4. Endpoint Detection and Response (EDR)? Product name:	Yes	No	N/A
a. What % of Endpoints are protected by above?			
b. What % of Servers are protected by above?			
5. Managed Detection and Response (MDR)? Product name:	Yes	No	N/A
6. Network Detection and Response (NDR)? Product name:	Yes	No	N/A
7. Security Information and Event Management (SIEM)? Product name:	Yes	No	N/A
a. If using Active Directory, are domain controller logs ingested by the SIEM?	Yes	No	N/A
b. What information does the SIEM ingest?			
c. What percentage of Applicant's "**Vital Assets**" are ingested by SIEM %			
d. How long does SIEM retain logs?			
8. Data Loss Prevention solution (DLP) in place? Product name:	Yes	No	N/A
a. Do alerts from the DLP feed into the SIEM?	Yes	No	N/A
b. Is your DLP solution email or network based?	Yes	No	N/A
c. Is your DLP solution in blocking mode?	Yes	No	N/A
9. Security Operations Center (SOC)? If 'Yes',	Yes	No	N/A
a. 24x7 live coverage with eyes on glass?	Yes	No	N/A
b. Internally staffed?	Yes	No	N/A
c. Managed by a third party?	Yes	No	N/A
d. Does the SOC have authority and ability to remediate security events?	Yes	No	N/A
e. Is the SOC provided an updated list of **vital assets** at least quarterly?	Yes	No	N/A
f. Of the products referenced in questions 1-8 of this section, which are monitored by the SOC?	Yes	No	N/A
IDS IPS EPP EDR MDR NDR SIEM DLP			
10. Regarding the products referenced in questions 1-8 of this section, are all that require updated definitions done at least daily?	Yes	No	N/A
11. Regarding the products referenced in questions 1-8 of this section, are all available anti-tamper features enabled?	Yes	No	N/A
12. Regarding the products referenced in questions 1-8 of this section, are all tools set to block suspected malicious activity vs. just notify?	Yes	No	N/A

	Yes	No	N/A
13. If the Applicant is using Active Directory, which of the following Audit Policies are enabled on Domain Controllers?	Yes	No	N/A
a. Audit Credential Validation (Failure)	Yes	No	N/A
b. Audit Process Creation (Success)	Yes	No	N/A
c. Audit Security Group Management (Success and Failure)	Yes	No	N/A
d. Audit User Account Management (Success and Failure)	Yes	No	N/A
e. Audit Other Account Management Events (Success and Failure)	Yes	No	N/A
f. Audit Sensitive Privilege Use (Success and Failure)	Yes	No	N/A
g. Audit Logon (Success and Failure)	Yes	No	N/A
h. Audit Special Logon (Success)	Yes	No	N/A
14. Implement a hardened baseline configuration materially rolled out across severs, laptops, desktops, and managed mobile device?	Yes	No	N/A
15. Employ vulnerability scanning across your enterprise?	Yes	No	N/A

   a. What % of the enterprise is covered?   %

   b. What is the frequency of scanning?

      Constant   Daily   Weekly   Monthly   > Monthly

	Yes	No	N/A
16. Route all outbound web requests through a web proxy which monitors for and blocks potentially malicious content?	Yes	No	N/A
17. Implement PowerShell best practices as outlined in the Environment Recommendations by Microsoft https://docs.microsoft.com/en-us/mem/configmgr/apps/deploy-use/learn-script-security	Yes	No	N/A
18. Segment your network based on certain criteria?	Yes	No	N/A

      The classification or level of information stored on your systems   By geography

      System criticality   Business function

      Subsidiaries   Brick and mortar locations

      Other:

	Yes	No	N/A
19. Segregate critical networks from internet facing or other less critical networks?	Yes	No	N/A
20. Do you segregate operational technology from information technology networks?	Yes	No	N/A
21. Configured host-based and network firewalls to disallow inbound connections by default?	Yes	No	N/A
22. An inventory of externally exposed assets?	Yes	No	N/A
23. Vulnerability scans of externally exposed assets?	Yes	No	N/A

   If 'Yes', what is the frequency?

      Constant   Daily   Weekly   Monthly   > Monthly

	Yes	No	N/A
24. Are Web Application Firewalls (WAF) in place for everything that is externally facing?	Yes	No	N/A
a. If 'Yes', is the WAF in blocking mode?	Yes	No	N/A
25. Protective DNS service (e,g., Quad9, OpenDNS or the public sector PDNS)?	Yes	No	N/A
26. On externally exposed systems, disable or block those ports, services, and protocols known to allow the spread of ransomware? These include, but are not limited to RDP, SMBv1, SMBv2	Yes	No	N/A

27. Penetration testing done by a third party?	Yes	No	N/A
a. If 'Yes', does the testing simulate known threat actor tactics, techniques, and procedures?	Yes	No	N/A
If 'Yes', what is the frequency?			

Annually   Semi-annually   Quarterly   Other

If the Applicant has any further comments on questions in the section above, please elaborate below:

EMAIL

1. What email platform is in use?			

Microsoft Office 365   Internal Microsoft Exchange

Google Workspace
                                          Other (please identify)

2. Multifactor Authentication (MFA) enabled on all user accounts?	Yes	No	N/A
3. Utilize an email monitoring/filtering solution (i.e. Microsoft ATP, Proofpoint, Mimecast)?	Yes	No	N/A
If 'Yes', enter solution.			
4. If 'Yes', does email monitoring/filtering solution perform any of the following?			
a. Blocks known malicious links, attachments, and suspicious file types, including executables	Yes	No	N/A
b. Blocks suspicious messages based on their content or attributes of the sender	Yes	No	N/A
c. Has the capability to run suspicious attachments in a sandbox	Yes	No	N/A
5. Implemented the following to protect against phishing messages:	Yes	No	N/A

SPF   DKIM and/or   DMARC

6. Conduct regular phishing simulations of staff? If so, how often:	Yes	No	N/A

Monthly   Quarterly   Annually

7. Measure-click through/fail rate? If Yes, please confirm:	Yes	No	N/A

0-5%   6-10%   11-16%   Higher fail rate

8. Is immediate additional training assigned for staff that fail phishing simulations?	Yes	No	N/A
9. Is access to web-based email such as Outlook Web Access permitted?	Yes	No	N/A
If 'Yes', is MFA enforced	Yes	No	N/A
10. Tag external emails to alert employees that the message originated from outside the organization?	Yes	No	N/A
11. Filter/scan incoming emails for malicious attachments and/or links?	Yes	No	N/A
If 'Yes', do you have the ability to automatically quarantine, detonate, and evaluate attachments?	Yes	No	N/A
12. Disable macros in office productivity software by default? (e.g., Microsoft Office, Google Workspace)	Yes	No	N/A
If 'Yes', are users allowed to enable macros?	Yes	No	N/A
13. Which legacy email protocols have been disabled?			

Basic Authentication   IMAP   POP3   SMTP

If the Applicant has any further comments on questions in the section above, please elaborate below:

PATCHING & SOFTWARE

	Yes	No	N/A
1. Have a patching policy in place to install critical and high severity patches across the enterprise? If so, please confirm the time frame:	Yes	No	N/A

        <24 hours   24-72 hours   2-7 days   7-30 days   >30 days

	Yes	No	N/A
a. Which systems are patched?			

        Internal servers   Workstations   Perimeter systems

	Yes	No	N/A
b. Is compliance with the policy tracked?	Yes	No	N/A

        i. If 'Yes', what is the compliance rate?

        >95%   90%-95%   80%-89%   <80%

	Yes	No	N/A
2. Have a patching policy in place to install normal severity patches across the enterprise? If so, please confirm the time frame	Yes	No	N/A

        24-72 hours   2-7 days   7-30 days   >30 days

a. Which systems are patched?

        Internal servers   Workstations   Perimeter systems   Third Party Apps   Web browsers

	Yes	No	N/A
3. Operate any end of life or end of support software or platforms?	Yes	No	N/A
a. If 'Yes', is it segregated from the rest of the network?	Yes	No	N/A
b. If 'Yes', is sensitive PII data stored or processed on these assets?	Yes	No	N/A
c. If 'Yes', do you purchase additional support for the software, where available?	Yes	No	N/A

If the Applicant has any further comments on questions in the section above, please elaborate below:

KNOWN VULNERABILITIES

	Yes	No	N/A
1. Has the Applicant been affected by any known vulnerabilities rated 10 or above in the common vulnerabilities and exposures database (https://nvd.nist.gov/general/nvd-dashboard)? (e.g. Keseya, Log4J, SolarWinds?)	Yes	No	N/A

    a. If 'Yes', please outline any and all patching procedures, mitigating controls, investigations, or evidence of malicious activity below, or provide in an appendix

BACKUPS & RECOVERY TIME

Does the Applicant:

	Yes	No	N/A
1. Conduct regular backup of data?	Yes	No	N/A

2. Frequently backup critical information? At least:

        Continuously   Daily   Weekly   Monthly   Quarterly   Semiannually   Annually

	Yes	No	N/A
3. Utilize physical backup tapes?	Yes	No	N/A

4. Store backups? Select all that apply:

        Cloud   On-premises   Offline storage   Off-site storage   Secondary data center

5. If "Cloud" was selected in Question 4:

a. Is your cloud-based backup service a "syncing service"? (e.g., DropBox, OneDrive, SharePoint, Google Drive)	Yes	No	N/A
b. Have you determined how long it would take to restore all data from the cloud?	Yes	No	N/A
c. Is access to cloud backups logged with alerts configured for suspicious activity?	Yes	No	N/A
d. Do you utilize versioning, data deletion prevention, and/or copies of the backups in other availability zones?	Yes	No	N/A

6. If "Offline storage" was selected in Question 4, is this done at least:

Daily   Weekly   Monthly   Quarterly   Other (please identify)

7. If "Off-site storage" was selected in Question 4, is this done at least:

Daily   Weekly   Monthly   Quarterly

8. Subject backups to the following measures? Select all that apply

Multifactor authentication   Encryption   Segmentation   Virus/malware scanning   Immutable

If "Encryption" was selected in Question 8, is there an offline backup of encryption keys?	Yes	No	N/A
9. Store unique backup credentials separately from other user credentials?	Yes	No	N/A
10. Employ a physical and logical separation of backups from the rest of the network?	Yes	No	N/A

If 'No', please outline the backup storage procedure:

11. Use unique accounts (not used for other systems) to access backups?	Yes	No	N/A
12. Use accounts that are domain joined to access backups?	Yes	No	N/A
13. Test a full recovery from a backup? If yes, the frequency of testing is at least:	Yes	No	N/A

Daily   Weekly   Monthly   Quarterly   Other (please identify)

14. Test the integrity of backups prior to restoration to be confident it is free from malware?	Yes	No	N/A
15. Maintain a warm or hot backup site for the purposes of resiliency, continuity, or redundancy?	Yes	No	N/A

16. What is the Applicant's average time to triage and contain security incidents of workstations year to date?

<30 minutes   30-120 minutes   2-8 hours   >8 hours   Other (please identify)

If the Applicant has any further comments on questions in the section above, please elaborate below:

NETWORK SECURITY ASSESSMENT

Does the Applicant:

1. Conduct security policy and procedure audits and remediate critical deficiencies?	Yes	No	N/A
2. Have physical security to control access to its data centers/server rooms? (e.g. 24 hr. guards, access cards, biometric access)	Yes	No	N/A
3. Replace factory default settings when configuring software and systems?	Yes	No	N/A
4. Enforce a clear desk policy at all sites?	Yes	No	N/A
5. Have an enterprise-wide data retention and destruction policy?	Yes	No	N/A
If 'Yes', is this policy regularly reviewed and updated?	Yes	No	N/A
6. Have antivirus protection in place and is it updated frequently?	Yes	No	N/A
7. Review antivirus software and firewalls, configurations, and settings on at least a quarterly basis?	Yes	No	N/A

8. Build information security measures into software that is developed or modified by internal resources?	Yes	No	N/A
9. Require all connecting devices to have antivirus and firewall installed?	Yes	No	N/A

If the Applicant has any further comments on questions in the section above, please elaborate below:

HANDLING & CRITICAL SENSITIVE INFORMATION (SENSITIVE INFORMATION AS DESCRIBED IN SECTION III.1. OF THIS APPLICATION)

Does the Applicant:

1. Have data classification/categorization measures in place?	Yes	No	N/A
2. Isolate critical/sensitive information in its own segregated environment?	Yes	No	N/A
3. Encrypt critical/sensitive information whilst at rest or in transit?	Yes	No	N/A
4. Use additional security measures such as tokenization or salting where applicable?	Yes	No	N/A

If the Applicant has any further comments on questions in the section above, please elaborate below:

MOBILE & PORTABLE DEVICES

Does the Applicant:

1. Encrypt all sensitive data that is physically removed from your premises by laptop, mobile/portable devices, USB, backup tapes or other means?	Yes	No	N/A
If 'Yes', do you require storage on mobile and portable devices to be encrypted?	Yes	No	N/A
If 'No', please confirm whether you allow information to be downloaded onto portable devices.	Yes	No	N/A
2. Allow Bring-Your-Own-Device (BYOD) connections to the business network? (If only allowed to connect to guest Wi-Fi, choose "No")	Yes	No	N/A
If 'Yes', does the Applicant have a policy that governs BYOD usage and controls?	Yes	No	N/A
3. Use a mobile device management system (MDM), which gives the ability to remote wipe the devices?	Yes	No	N/A
If 'Yes', is the MDM system applied to: Company-owned devices "BYOD" devices minutes			
4. Encrypt sensitive data when sent outside of its network (in transit)?	Yes	No	N/A

If the Applicant has any further comments on questions in the section above, please elaborate below:

DATA RECOVERY & NETWORK BUSINESS INTERRUPTION ASSESSMENT

Does the Applicant:

1. Have any of the following plans in place to address security or data breaches:			
Incident response plan Business continuity plan Disaster recovery plan			
a. If 'Yes', do the plan(s) clearly define the responsibilities and the support personnel for each key role?	Yes	No	N/A
b. If 'Yes', does the plan(s) include ransomware-specific response and recovery plans?	Yes	No	N/A
c. If 'Yes', are the plan(s) tested at least annually with any critical deficiencies remediated?	Yes	No	N/A
d. If 'Yes', are the plan(s) readily available in hardcopy?	Yes	No	N/A

2. Conduct cybersecurity incident tabletop exercises?	Yes	No	N/A
a. Approximate date of last exercise?			
b. Did the exercise include a threat from ransomware?	Yes	No	N/A
3. Track how long it takes to restore the Applicant's **vital assets** following a network outage? If so, the length of time is:	Yes	No	N/A

Less than 8 hours	Between 8 and 12 hours	Between 12 and 24 hours	Between 24 and 72 hours	More than 72 hours

4. Track how long it takes to restore the Applicant's non-critical systems following a network outage? If so, the length of time is:	Yes	No	N/A

Less than 8 hours	Between 8 and 12 hours	Between 12 and 24 hours	Between 24 and 72 hours	More than 72 hours

5. What is the Applicant's Recovery Time Objective (RTO)?			
a. Does the Applicant test and meet the RTO?	Yes	No	N/A

If the Applicant has any further comments on questions in the section above, please elaborate below:

LEGAL & REGULATORY

Does the Applicant:

Have policies and procedures in place covering the following individuals' rights under countries' data protection regulations?	Yes	No	N/A
1. Individuals are informed about the collection and use of their personal data	Yes	No	N/A
2. Individuals have the right to access their personal data and a formal subject access request process is in place	Yes	No	N/A
3. Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete, and a formal data rectification request process is in place	Yes	No	N/A
4. Individuals have the right to have personal data erased and a formal data erasure process is in place	Yes	No	N/A
5. Individuals have the right to obtain and reuse their personal data for their own purposes across different services and a formal data portability policy is in place	Yes	No	N/A
6. Individuals have the right to object to the processing of their personal data and a formal objection policy is in place	Yes	No	N/A
7. Have a lawful basis to carry out profiling and/or automated decision-making which is documented in our data protection policy	Yes	No	N/A
8. Have a privacy policy?	Yes	No	N/A
If 'Yes'			
a. Is the privacy policy displayed on the Applicant's website?	Yes	No	N/A
b. Is the privacy policy approved by the Applicant's Board or legal department?	Yes	No	N/A
c. Is the privacy policy regularly reviewed and updated?	Yes	No	N/A
9. Have a written, Board-approved policy that addresses compliance with applicable privacy and security laws or regulations?	Yes	No	N/A

If you have answered 'No' to any of the questions above, please provide an explanation and information on your plans for compliance below:

If the Applicant has any further comments on questions in the section above, please elaborate below:

VENDOR MANAGEMENT

1. Please identify all vendors that have access to or help to manage the Applicant's network or security systems:

Name of vendor	Nature of service	Does the vendor indemnify the Applicant under contract?		
	Data center hosting	Yes	No	N/A
	Cloud services	Yes	No	N/A
	Web hosting	Yes	No	N/A
	Critical software	Yes	No	N/A
	Managed security services	Yes	No	N/A
	Data processing services	Yes	No	N/A
	Endpoint detection and response	Yes	No	N/A
	Antivirus	Yes	No	N/A
	Firewall	Yes	No	N/A
	Intrusion detection and prevention systems	Yes	No	N/A
	Internet service provider	Yes	No	N/A
	Data loss prevention	Yes	No	N/A
	Recovery services	Yes	No	N/A
	Other (please state):	Yes	No	N/A

2. Are all vendors required to comply with the Applicant's security policy?	Yes	No	N/A
3. Are vendors audited to ensure that they meet the Applicant's security and privacy standards as well as those customary in the relevant industry and those mandated by regulators?	Yes	No	N/A
4. Are vendor access rights periodically reviewed and updated?	Yes	No	N/A
5. Is vendor access on the Applicant's network monitored?	Yes	No	N/A
6. Is vendor access limited to dedicated time windows?	Yes	No	N/A
7. Does the Applicant periodically review all contracts to ensure that they satisfy data security and privacy laws and regulations?	Yes	No	N/A
8. Does the Applicant have a procedure to manage the termination of vendor contracts?	Yes	No	N/A
9. Does the Applicant require vendors to have cyber insurance coverage?	Yes	No	N/A

If the Applicant has any further comments on questions in the section above, please elaborate below:

BIOMETRIC INFORMATION

Does the Applicant:

1. Collect, store, process, use or retain any biometric information? If yes, please complete the following section.	Yes	No	N/A

2. Collect, receive, or retain any biometric data on employees or consumers as defined by law including (but not limited to):

Retina scan   Voiceprint   Iris scan   Hand scan   Fingerprint   Face geometry   Other (please identify)

3. Clearly define to employees, consumers, and/or individuals how the Applicant will:

Collect their biometric information   Use their biometric information   Destroy their biometric Information

4. Sell, lease, trade or otherwise profit from the biometric information of employees/consumers/individuals?	Yes	No	N/A

5. Subject biometric information to the following measures? Select all that apply.

Encryption in transit   Restricted access a least **privileged** basis   Encryption at rest

Segregated in an isolated environment   Other (please identify)

6. Obtain written consent from employees/consumers/individuals prior to collection, receipt, or retention of biometric data?	Yes	No	N/A
7. Have a retention schedule outlining how long biometric information is retained?	Yes	No	N/A
8. Have a data destruction policy for biometric information that is no longer required?	Yes	No	N/A
9. Has the Applicant received any complaints alleging the unlawful collection, use, dissemination, or sale of biometric data? If 'Yes', please describe:	Yes	No	N/A

If the Applicant has any further comments on questions in the section above, please elaborate below:

PAYMENT CARD INDUSTRY ASSESSMENT

(complete only if applying for PCI DSS liability coverage)

Does the Applicant:

1. Accept payment cards for its goods or services?	Yes	No	N/A
If 'Yes', is the Applicant compliant with PCI DSS Security Standards?	Yes	No	N/A

If 'No', please describe the current status of the Applicant's compliance work:

a. What Level of PCI Merchant is the Applicant?

b. Approximately how many transactions were processed during the last 12 months?

c. What is the approximate percentage of annual revenue attributable to credit card transactions?   %

2. Store payment card data on its network?	Yes	No	N/A

If 'Yes':

a. For how long is such data stored on the Applicant's network?

b. Is payment card data either encrypted or tokenized at all times?	Yes	No	N/A

c. If the payment card data is not encrypted or tokenized, please describe what security protects such data
   in an appendix to this application.

3. Transact all payments through a payment processor?	Yes	No	N/A

If 'Yes':

a. Who is the payment processor?

b. Has the payment processor provided evidence of its PCI DSS compliance to the Applicant?	Yes	No	N/A
4. Are 100% of your point to sale terminals EMV compliant?	Yes	No	N/A

If the Applicant has any further comments on questions in the section above, please elaborate below:

MULTIMEDIA ASSESSMENT

(Complete only if applying for multimedia liability coverage)

Does the Applicant:

1. Have a process in place to review media content (website, social media or otherwise) for the following prior to publication?

a. Infringement of copyright?	Yes	No	N/A
b. Infringement of trademark?	Yes	No	N/A
c. Libel or slander?	Yes	No	N/A
d. Invasion of privacy?	Yes	No	N/A
2. Require a qualified attorney to review the above?	Yes	No	N/A

If 'No', please describe the procedures to avoid the posting of improper or infringing content:

3. Have a procedure for responding to any allegations which are in the nature of items 1. (i) to (iv) above?	Yes	No	N/A
4. In respect of the Applicant's website:			
a. Does the Applicant record visitor acceptance of terms of use before access is granted?	Yes	No	N/A
b. Does the website include third-party content?	Yes	No	N/A
If 'Yes':			
i. Does this content include streaming video and music?	Yes	No	N/A
ii. Does the Applicant have procedures in place to secure rights for using all such third-party content?	Yes	No	N/A

c. Does the Applicant allow third parties to post content directly to the website?		Yes	No	N/A
d. Does the Applicant monitor content for offensive, harassing, infringing or other undesirable material?		Yes	No	N/A
e. Does the Applicant reserve the right to remove or censor any content that violates the Applicant's acceptable terms of use?		Yes	No	N/A

If the Applicant has any further comments on questions in the section above, please elaborate below:

Advertising activities

1. Marketing/advertising costs

	Past fiscal year	Current fiscal year	Next fiscal year
U.S. costs			
Non-U.S. costs			
Total costs			

2. Advertising channels: Please indicate the approximate percentages of advertising/marketing spending in each of the following channels:

Television/cable	%	Direct mail/catalog (print)	%
Newspapers (print)	%	Digital/online (all channels)	%
Magazines (print)	%	Other, please describe:	%

3. Have a procedure for responding to any allegations which are in the nature of items 1. (i) to (iv) above?	Yes	No	N/A
4. How many trade or service marks does the Applicant currently own?			
5. For the proposed policy period, does the Applicant plan to use any of the Applicant's existing trade or service marks in connections with any new class(es) of goods or services for which the marks have not previously been used?	Yes	No	N/A
6. Does the Applicant engage outside counsel specializing in trademark law in connections with the development or use of the Applicant's marks and products?	Yes	No	N/A
7. Does the Applicant always perform trademark clearance searches in connection with new marks or when expanding into new classes of goods or services?	Yes	No	N/A
8. Does the Applicant operate an in-house advertising agency? (i.e., does the Applicant create advertising and/or marketing content internally)?	Yes	No	N/A
9. Does the Applicant employ outside advertising agencies to create advertising or marketing content?	Yes	No	N/A
10. Does the Applicant utilize a website or social media to advertise or promote its products or services?	Yes	No	N/A
11. Does the Applicant have a written employee social media policy?	Yes	No	N/A
12. Does the Applicant have a process for legal review of all advertising, marketing, and promotional content, including website and social media content, prior to dissemination?	Yes	No	N/A
13. Has the Applicant ever received notification that any of its advertising, marketing or promotional content infringes on the intellectual property rights of others?	Yes	No	N/A

If the Applicant has any further comments on questions in the section above, please elaborate below:

Media risk control & legal review

1. When providing technical, health-related or DIY related advice or guidance, does the Applicant always use a disclaimer or other warning?	Yes	No	N/A
2. Does the Applicant have formal, written policies and procedures for addressing requests to remove allegedly offensive or infringing content disseminated by or on behalf of Applicant?	Yes	No	N/A
3. Does the Applicant permit any User Generated Content ("UGC"), whether in the form of comments, videos, audio recordings, photographs/images, or other content, to be uploaded or shared on any of Applicant's websites or mobile apps?	Yes	No	N/A

4. Please indicate which of the following additional quality control/risk management procedures the Applicant uses in connection with the Applicant's media activities (select all that apply):

Website/social media content conduct and policy

Delay device used for live transmissions / broadcasts

Regular training of employees regarding libel and related claims

Regular training of employees regarding copyright, trademark, and other content claims

Other (please identify)

If the Applicant has any further comments on questions in the section above, please elaborate below:

TECHNOLOGY E&O (INCLUDING MISCELLANEOUS PROFESSIONAL LIABILITY)

(complete only if applying for technology errors and omissions coverage)

1. Please provide a percentage breakdown of the Applicant's annual revenue between the following activities:

Services and products	Industries served	Estimated % of revenue	Length of time sold or provided
Hardware			
a. Sales of own brand			
b. Distribution of other brands			
c. Installation			
d. Maintenance			
Software product sales			
a. Sales of own brand shrink wrapped/off the shelf software			
b. Distribution of other brand shrink wrapped/off the shelf software			
a. Customizable software			

Services and products	Industries served	Estimated % of revenue	Length of time sold or provided
Software services			
a. Installation, including configuration (no coding involved)			
b. Customization (including coding changes)			
c. Maintenance			
d. Systems integration			
e. End-user applications			
Services and products			
a. Consultancy			
b. Contract staff			
c. Support services			
d. Project management			
e. Training			
f. Data management/ processing			
g. Data communication services			
h. Internet service provision of hosting			

2. Please indicate the Applicant's five largest contacts/ projects:

Client	Product/service	Contract revenues for this year/total contract value

3. Does the Applicant provide professional services other those described above to customers or clients? Yes No N/A

If 'Yes', please describe:

a. What percentage of your revenues are derived from such professional services?   %

4. What percentage of your work is performed by subcontractors?   %

5. Operations controls

   a. Does the Applicant have written contracts with all clients the Applicant performs work for or provides products to?   Yes   No   N/A

   If 'No', what percentage (%) of the time are they used?   %

   b. Do all services contracts with customers fully describe the scope of services to be provided?   Yes   No   N/A

   c. Do all contracts include how any disputes between the Applicant and the customer will be handled?   Yes   No   N/A

   d. Do all services and products contracts include provisions for the following:

      i. Damages caps: Yes   No   N/A

        If 'Yes', what is the standard cap on damages?

      ii. Disclaimer of implied warranties   Yes   No   N/A

      iii. Guarantees   Yes   No   N/A

      iv. Full disclaimer of consequential damages   Yes   No   N/A

If the response to Question 3.d.iv. is 'No', please explain the circumstances when a full disclaimer of consequential damages is not provided:

Contractual procedures & controls

1. Does the Applicant require the use of written contracts for all engagements?   Yes   No   N/A

2. What is the average length and value of the Applicant's contracts?

3. Does the Applicant have a contractual review process?   Yes   No   N/A

4. Please indicate the percentage of contracts used that are:

   Applicant's standard contract: % Customers' contracts: % Customized or combination: %

5. Which of the following contractual provisions does Applicant always strive to impose in its favor in written contract (select all that apply)?

Disclaimer of warranties	Indemnification/hold harmless
Alternative dispute resolution	Limitation of liability
Exclusion of consequential damages	Performance milestones
Exclusive remedies for breach	Statement of work (SOW)
Force majeure	Choice of law or venue

6. Does the Applicant have a formal customer acceptance of work/project completion process?   Yes   No   N/A

7. Are performance milestones required to be accepted with signoff/approval by both parties?   Yes   No   N/A

8. Are interim changes to SOWs or contracts documented and approved by both parties?   Yes   No   N/A

9. Please describe the person by title or position employed by Applicant who have authority to alter or amend Applicant's standard contract language:

10. How many open/ongoing customer complaints/disputes is the Applicant currently handling?

Quality control/risk management procedures

1. Does the Applicant employ a Risk Manager?	Yes	No	N/A

If you answered 'No' above, who is responsible for handling insurance-related matters?

2. Does the Applicant have written policies and procedures for responding to customer complaints?	Yes	No	N/A
3. Does the Applicant have an escalation procedure to respond to customer complaints?	Yes	No	N/A

4. Which of the following quality control procedures does Applicant employ (select all that apply)?

Alpha testing	Customer support by email or text
Beta testing	Formalized training for new employees
Business continuity plan	Prototyping with testing
Customer screening process	Vendor certification and management procedures
Customer support by telephone	Written quality control standards and procedures
Customer support by web portal	Other (please describe below):

CYBER CRIME/SOCIAL ENGINEERING

(complete only if applying for cyber/social engineering coverage)

Does the Applicant:

1. Make payments to third parties by wire transfers?	Yes	No	N/A

If 'Yes':

a. How many times per week?

b. What is the most common amount transferred?

c. Do payments or transfers of a certain amount require dual authorization?	Yes	No	N/A
2. Have procedures in place to verify the receipt of goods or services against an invoice prior to payment?	Yes	No	N/A
3. Call a vendor using known prior telephone number to confirm any changes in bank account info, invoice amounts, location, contact number, fax number, etc.?	Yes	No	N/A
4. Accept payments or funds transfer instructions from a customer or client relating to a refund or repayment of goods or services?	Yes	No	N/A

If 'Yes', what methods of receiving instructions are deemed acceptable (e.g. phone call, email, text message)?

5. Confirm all payments or funds transfers from a customer or client by a direct call to the customer or client using a previously known telephone number?	Yes	No	N/A
6. Have procedures in place to verify the authenticity of any payment request made by an internal company source (another employee, etc.)?	Yes	No	N/A
7. Had any social engineering losses? If 'Yes', please describe.	Yes	No	N/A

III. Claims & insurance history

CLAIMS

In the last five (5) 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 and/or does the Applicant 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   N/A

If 'Yes', please provide details in an appendix to this application.

INSURANCE HISTORY

1. During the last five (5) years, has any insurance policy providing substantially the same or similar insurance as the insurance being applied for under this application been declined, canceled or nonrenewed at the choice of the insurer?

Yes   No   N/A

2. Does the Applicant currently have insurance in place covering privacy or data security exposures?

Yes   No   N/A

If 'Yes', please confirm:

Insurer	Aggregate policy limit	Self-insured retention	Inception date	Expiry date	Retroactive date	Premium

IV. Declaration

The undersigned authorized representative of the Applicant declares that the statements set forth herein are true. The signing of this application does not bind the undersigned or the insurer to complete the insurance. It is represented that the statements contained in this application and the materials submitted herewith are the basis of the contract should a policy be issued and have been relied upon by the insurer in issuing any policy. The insurer is authorized to make any investigation and inquiry in connection with this application as is reasonable and necessary. Nothing contained herein or incorporated herein by reference shall constitute notice of a claim or potential claim so as to trigger coverage under any contract of insurance.

This application and materials submitted with it shall be retained on file with the insurer and shall be deemed attached to and become part of the policy if issued. It is agreed in the event there is any material change in the answers to the questions contained in this application prior to the effective date of the policy, the Applicant will notify the Insurer in writing and any outstanding quotations may be modified or withdrawn at the insurer's discretion.

Must be signed by a corporate officer with authority to sign on the Applicant's behalf.

Signed:

Title:

Print name:

Date:

SUPPLEMENT A — HEALTHCARE ASSESSMENT

1. Is the Applicant compliant with HIPAA?	Yes	No	N/A

2. When was the Applicant's compliance with HIPAA last reviewed?

3. Does the Applicant host or use a healthcare exchange to share data with other healthcare organizations?	Yes	No	N/A

If 'Yes', please describe what data is being shared and with whom:

SUPPLEMENT B — OPERATIONAL TECHNOLOGY (E.G., SCADA, DCS, CIM, CNC, ETC.)

1. Please provide an overview of the Operational Technology (OT) on your network:

2. Please provide an overview of the team responsible for OT and their reporting structure:

3. Do you employ a dedicated OT cyber security professional?	Yes	No	N/A
4. Do you maintain an up-to-date inventory of all IT and OT assets identifying 100% of your assets?	Yes	No	N/A

   a. If not 100% please estimate the percentage of OT assets inventoried as well as any compensating controls for non-inventoried assets   %

5. What is the highest dependency you have on any one facility?

6. What percentage of maximum capacity is your production facility running?   %

7. In the event of an outage, can you make up the lost production at the facility affected by adding shifts or running at a higher capacity at this or another facility?	Yes	No	N/A

8. How many days of finished inventory do you hold at your production facility or distribution warehouse?

9. Does the Applicant utilize the following technologies to physically or logically segregate your IT and OT networks?

   Air Gap   DMZ   Firewall   VLAN

If VLAN is selected, please describe the degree to which traffic is restricted and what technical control is used to enforce segmentation.

10. Do all OT assets using legacy software (e.g., Windows XP) have enhanced security?	Yes	No	N/A
11. Is MFA required for remote access to OT environment?	Yes	No	N/A

   a. If 'No', describe any additional security in place

12. Are the following in place to further secure your OT environment?

Application whitelisting	Disabled removable devices
Managed security patching	Intrusion detection systems
Intrusion prevention system	SIEM
Endpoint protection	Third-party penetration testing

13. Have all default usernames and passwords in the OT environment been removed/modified?	Yes	No	N/A
14. Do you allow remote access to OT environment?	Yes	No	N/A

If 'Yes', what security is in place:

15. Is the use of removable devices (e.g., USB memory sticks) disabled within the OT environment?	Yes	No	N/A

If 'No', what security is in place:

16. Is the use of removable devices (e.g., USB memory sticks) disabled within the OT environment?	Yes	No	N/A

a. Why are these systems still in place?

b. Are there any compensating controls in place to mitigate the risk?

c. What plans exist to upgrade or remove these systems?

17. Do you prevent browsing the Internet and checking email on industrial systems?	Yes	No	N/A
18. Is OT restoration explicitly addressed in your disaster recovery plan?	Yes	No	N/A
19. Are your OT environments included in your backup strategy?	Yes	No	N/A

Please describe any difference between how they are stored and other backups

SUPPLEMENT C — PRIVILEGED SERVICE ACCOUNT APPENDIX

Name of account	Privileges it has	Software product it supports	What hosts it authenticates to	Why are the privileges required

Please use separate document if additional space is needed for more accounts.

LOCKTON®

UNCOMMONLY INDEPENDENT