CYBER-POLICY-QUESTIONNAIRE

1. Company Information

1a. Company Name

1b. How many employees does your organization have?

1c. Which cloud infrastructure platforms[1] do you leverage? **Check all that apply**

- [ ] **Microsoft Azure**
- [ ] **Amazon AWS**
- [ ] **Cloud based backups**
- [ ] **Google Cloud Platform**
- [ ] **No cloud infrastructure platform**
- [ ] **Other cloud infrastructure platform**

1d. How do you manage your IT and security infrastructure? **Check all that apply | List all applicable vendors**

- [ ] **Internal IT team**
- [ ] **Internal security team**
- [ ] **Managed Service Provider (MSP)**
- [ ] **Managed Security Service Provider (MSSP)**
- [ ] **Managed Detection and Response (MDR)**
- [ ] **No dedicated IT team**
- [ ] **No dedicated security team**
- [ ] **Other**

2. Email Security

2a. Do you have email filtering in place? ◉ Yes ○ No

If "Yes", list the name of your email filtering solution.

Do you use an advanced email security solution that includes features such as URL and attachment sandboxing. (Secure Email Gateway) ○ Yes ○ No

If "Yes", please list the name of your solution.

If "No", which of the following features are enabled in your email filtering solution? **Check all that apply**

- ☐ **Spam and phishing protection**
- ☐ **User impersonation protection**
- ☐ **Attachment sandboxing**
- ☐ **URL sandboxing**
- ☐ **Blocking executable file attachment extensions (e.g. .exe, .bat, .vbs)**
- ☐ **Blocking macro enabled Microsoft Office documents**

2b. Do you enforce Multi-Factor Authentication (MFA) for email access via webmail portal (i.e. Gmail), mailbox applications (i.e. Outlook Application) and non-corporate devices for all employees? ○ Yes ○ No

2c. How often do you conduct phishing training?

○ **Ad-hoc**	○ **Semi-Annually**	○ **Never**
○ **Quarterly**	○ **Annually**	○ **Yes, frequency unknown**

3. Data Backup & Recovery

3a. Do you have a backup solution? (●) Yes ( ) No

If "Yes", how frequently do you back up systems and data?

( ) Continuous backups ( ) Weekly ( ) Less than monthly

( ) Daily ( ) Monthly ( ) Never

Which systems are included in your backup strategy? **Check all that apply**

- [ ] Business critical systems
- [ ] All servers
- [ ] All workstations
- [ ] SaaS applications
- [ ] No systems
- [ ] Other systems

Which of the following are in place for your backup solution(s)?

- [ ] Backup servers are segmented from the rest of the network
- [ ] Copy of backups are kept offline or air-gapped
- [ ] Cloud based backups
- [ ] Multiple copies of backups stored in 2 or more geographical locations
- [ ] MFA required for access to backups files (on-premise and cloud)
- [ ] Backup solution with immutable backups
- [ ] Backup servers are not joined to a Windows domain
- [ ] Backup servers and user accounts leverage unique credentials
- [ ] Backups are encrypted
- [ ] Other Controls (Describe your current backup process and solution):

3b. Do you have a Business Continuity Plan (BCP) or Disaster Recovery Plan (DRP) in place?

◯ Yes ◯ No

3c. How frequently do you test the integrity of your backups and your disaster recovery plan?

◯ Monthly ◯ Quarterly ◯ Bi-annually ◯ Annually ◯ Untested

◯ Other frequency

4. Privileged Account Management

4a. How are privileged accounts[2] secured and managed?

☐ Administrative users use different accounts for administrative use and non-administrative use (e.g. day to day activities such as web browsing and email)

☐ Standard users do not have administrative rights to their workstations

☐ Local administrator accounts are unique and complex on all systems

☐ A password management vault is used to manage privileged accounts

☐ Multi-Factor Authentication used to secure and manage internal use of privileged accounts (administrator accounts, service accounts, etc.)

☐ No controls

☐ Other Controls

5. Endpoint & Network Security

5a. What remote access is present that allows for users to connect into the environment while outside of the office?

Check all that apply | List all applicable vendors

- [ ] Remote Desktop (RDP)
- [ ] Citrix
- [ ] Virtual Private Network (VPN)
- [ ] Remote access software (e.g. LogMeIn)
- [ ] No remote access
- [ ] Other remote access

5b. Do you enforce Multi-Factor Authentication to secure all remote access to your network?

○ Yes ○ No ○ N/A

5c. What Endpoint Security Technology do you have in place? (check all that apply)

- [ ] Standard Antivirus
- [ ] Next Gen Antivirus
- [ ] Endpoint Protection (EPP) across your enterprises
- [ ] Endpoint Protection & Response (EDR) across your enterprises
- [ ] Managed Detection & Response (MDR) across your enterprises
- [ ] Extended Detection & Response (XDR) across your enterprises
- [ ] Other

5d. Does your organization have established processes for applying security updates across servers, laptops, desktops and managed mobile devices? ◯ Yes ◯ No

If "Yes", please check the corresponding timeframe in which critical security updates are typically applied.

◯ 24 - 48 Hours ◯ 7 - 14 Days ◯ 30+ Days

◯ 2 - 6 Days ◯ 15 - 29 Days

6. Data Security

6a. Where does sensitive data reside in the environment[3]? **Check all that apply | List all applicable vendors**

- ☐ Mobile devices
- ☐ User workstations
- ☐ On-premise servers
- ☐ Cloud Platform (AWS, Azure, GCP)
- ☐ SaaS Providers (HR systems, Payroll, etc.)
- ☐ No sensitive data
- ☐ Other

6b. What security controls are in place to protect against unauthorized access to sensitive and confidential data?

Check all that apply

- ☐ Role-based access control leveraging the principle of least privilege
- ☐ Network segmentation of servers containing sensitive data
- ☐ MFA required for all user access to systems/applications with sensitive data
- ☐ Logging and monitoring
- ☐ No security controls
- ☐ Other security controls

6c. How is sensitive data encrypted across systems and devices? **Check all that apply**

- [ ] **No encryption**
- [ ] **Mobile Device encryption (eg cell phones, laptops, etc.)**
- [ ] **Encryption at Rest (File Level)**
- [ ] **Encryption for Data in-transit**
- [ ] **Other encryption methods**

Warranty

All Insureds agree that the statements contained herein are their agreements and representations, which shall be deemed material to the risk, and that, if issued, the Policy will be in reliance upon the truth thereof. The misrepresentation or non-disclosure of any material matter by the Insured or its agent will render the Policy null and void and relieve the Company from all liability under the Policy.

Applicant Signature | Print Name | Date

Footnotes

[1] Cloud infrastructure platforms refers to leveraging a third party provider to host servers, services, or applications in a cloud environment. This does not include Software as a Service (SaaS) platforms like email or other business productivity tools.

[2] Privileged accounts refer to accounts that have administrator permissions on systems or applications. This commonly includes local administrator, domain administrator, and service accounts.

[3] This applies to areas where sensitive data is centrally located or has a high likelihood of being stored during the normal course of business (e.g. if users download sensitive data to their local systems).