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
- [ ] 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

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. Email Security

2a. Do you enforce Multi-Factor Authentication (MFA) for access to emails for all employees?

◯ Yes ◯ No

2b. What email security solution (vendor) do you use?

2c. Which of the following features are enabled in the email security 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

2d. How often do you conduct phishing training?

◯ Ad-hoc ◯ Quarterly ◯ Semi-Annually ◯ Annually ◯ Never

3. Data Backup & Recovery

3a. 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

3b. How frequently do you back up systems and data?

◯ Continuously ◯ Daily ◯ Weekly ◯ Monthly ◯ Never
◯ Other frequency

3c. Which solutions are a part of your backup strategy?

CHECK ALL THAT APPLY | LIST ALL APPLICABLE VENDORS

- ☐ On-site backup software *(e.g. Veeam, Dell, Commvault)*
- ☐ Off-site backup *(e.g. tape, AWS S3, Azure Blob storage)*
- ☐ Backup as a Service *(e.g. Veeam Cloud Connect, Druva, Acronis)*
- ☐ No solutions
- ☐ Other solutions

3d. How are local backups protected against deletion or corruption?

CHECK ALL THAT APPLY

- ☐ MFA required for access to the backup management interface
- ☐ MFA required for access to backup files *(on-premise and cloud)*
- ☐ Backup servers are not joined to a Windows domain
- ☐ Backups servers and user accounts leverage unique credentials
- ☐ Backup servers are segmented from the rest of the network
- ☐ Backup solution with immutable backups
- ☐ Copy of backups are kept offline or air-gapped
- ☐ No protection
- ☐ Other controls

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

◯ Yes ◯ No

3f. 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?

CHECK ALL THAT APPLY

- [ ] Administrative users use different accounts for administrative use and non-administrative use *(e.g. day to day activities)*
- [ ] 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
- [ ] MFA required for internal use of privileged accounts *(e.g. when used for internal RDP connections)*
- [ ] 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 (MFA) to secure all remote access to your network?

◯ Yes ◯ No

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

5c. What Endpoint Security Technology do you have in place?

CHECK ALL THAT APPLY

Standard Anti-virus

- [ ] McAfee MVISION Endpoint Security
- [ ] Symantec Endpoint Security
- [ ] Webroot Endpoint Protection
- [ ] Malwarebytes
- [ ] Microsoft Defender *(standard built-in anti-virus)*
- [ ] No standard anti-virus
- [ ] Other standard anti-virus

Next-Gen Anti-virus

- [ ] Cylance
- [ ] CrowdStrike Falcon Protect
- [ ] SentinelOne Singularity Core
- [ ] Sophos Intercept X Advanced
- [ ] No next-gen anti-virus
- [ ] Other next-gen anti-virus

Endpoint Detection & Response

- [ ] CrowdStrike Falcon Insight
- [ ] SentinelOne Singularity Complete
- [ ] Sophos Intercept X Advanced with XDR
- [ ] FireEye Endpoint Security
- [ ] Microsoft Defender for Endpoint
- [ ] VMware Carbon Black Endpoint
- [ ] No endpoint detection
- [ ] Other endpoint detection

Other endpoint security technology

5d. What Network Security Technology is in place?

CHECK ALL THAT APPLY | LIST ALL APPLICABLE VENDORS

- [ ] Traditional Firewall
- [ ] Next-Gen Firewall
- [ ] Intrusion Detection / Prevention System *(IDS/IPS)*
- [ ] Secure web gateway / Web proxy / network filtering
- [ ] Protective DNS
- [ ] CASB / SASE
- [ ] No network security
- [ ] Other network security

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
- [ ] Logging and monitoring
- [ ] No security controls
- [ ] Other security controls

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)*.

6c. How is sensitive data encrypted across systems and devices?

CHECK ALL THAT APPLY

- ☐ Full disk encryption *(e.g. laptops)*
- ☐ Mobile device encryption *(e.g. cell phones)*
- ☐ File level encryption
- ☐ Data in-transit
- ☐ No encryption
- ☐ 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.

Print Name	Signature	Date