

Cyber Liability Insurance Questionnaire

1. Name of Insured

2. Business Operations Address (Physical)

3. Description of Business Operations

4. Website Address

5. Number of Employees

6. Project Gross Revenue

(Next 12 Months)

7. Do you enforce MFA on the following?

All remote access to corporate email

All remote access to eligible systems
(laptops, desktops, workstations, servers)

All remote access to corporate networks (including
VPNs)

All remote access to backups of sensitive/business
critical data

All access by privileged users

8. Which of the following Inbound Email Security products (SEG) products does the applicant use, if any?

Appraver	Avanan	Barracuda	Darktrace	Datto	Inky	Google	Intermedia
Ironscales	Mimecast	Microsoft Defender for O365	Perception Point	Proof-point	Vade	Other/Unknown	None of the Above

9. The applicant uses the following tool to protect network Endpoints from malware:

Anti-virus (signature based)	Next gen anti-virus (ngav)	Endpoint protection platform (epp)	None
Endpoint protection & response (edr)	Managed detection & response (mdr)	Extended detection & response (xdr)	Don't know

10. How often do you conduct employee security training or phishing training?

Ad-hoc	Semi-Annually	Never
Quarterly	Anually	

11. Do you have a backup solution?

How frequently do you back up systems and data?

Continuously	Weekly	Less than Monthly
Daily	Monthly	Never

12. Desired Limits _____

13. Have there been any claims? Yes No

Signature: _____

Date: _____