



Netsafe Short Form Cyber Application

General Information

Name of Applicant (Insured Organization):			
Address:			
City:	State:	Zip:	Telephone:
Date Established:		State of Incorporation:	
Website:			
Revenues:			

Type of Private Information	Estimated Number of Records
Personal Identifiable Information (PII) - (i.e. - Social Security, Customer Info. or Biometric Data)	
Personal Healthcare Information (PHI) - (i.e. – Medical Records, Health Insurance Account)	
Financial Information - (i.e. – Credit Cards, Bank Account Information, Money/Securities)	
Third Party Corporate Information - (i.e. – Non - Disclosure Contract)	<input type="checkbox"/> Yes <input type="checkbox"/> No

GOVERNANCE CONTROLS

- Are you subject to any Regulations – Biometric Data Law, GDPR, CCPA or HIPPA? Yes No
If yes, are you compliant including protocols to prevent the wrongful collection of Private Information? Yes No
- Does your organization have a Written Information Security Policy (WISP) and/or Privacy Policy? Yes No
- Vendor Risk Management Protocols - Cyber Risk Controls and Contractual Language? Yes No
- Is the Applicant compliant with Payment Card Industry Data Security Standards (PCI-DSS)? N/A Yes No
- Have an employee-training program relating to Cyber Risk, including Phishing? Yes No

SECURITY CONTROLS

- How many network capable endpoints (computers or mobile devices) does the Applicant have in their care, custody or control?
- What is the approximate total dollar values of the computer system?
- Do you have Firewalls? Yes No
- Do you have Anti-Virus – Static or Heuristic? Yes No
- Encryption tools on Private Information – At Rest, In-Transit and/or Mobile Devices Yes No
 - If possible, please provide some information around your encryption policy/procedure (Optional):
- End-Point Detection/Response (EDR) or Intrusion Detection/Prevention (IDR) Tool? Yes No
- Conduct Vulnerability Scanning and Patching for all platforms or applications? Yes No
If yes, how often:

13. Do you have Multi-Factor Authentication enforced on the following platforms:
- a. Privileged User Accounts Yes No
 - b. Remote Access – Remote Desktop, Virtual Private Network, Virtual Desktop Infrastructure Yes No
 - c. Email, including Office 365, G-Suite or other provider Yes No
 - d. Critical platforms or applications to operate the business Yes No
 - e. Critical platforms or applications that handle Private Information Yes No
 - f. Backups or Recovery Yes No
14. Do you have an email filtering tool including the ability to pre-screen, external source identification, attachments and links evaluation, quarantine, sandbox or automatic detonation of malicious emails? Yes No
15. Do you take regular backups of all organizational critical platforms, applications or information? Yes No
- If yes:
- a. Are the backups encrypted? Yes No
 - b. Is recovery of critical platforms, applications or information from backups documented? Yes No
 - c. Are backups stored in a secure location (separate from network or system)? Yes No
 - d. How frequently is data backed up?
 - e. How often is the recovery from backups being tested?
 - f. Recovery Time Objective (RTO) to restore from backups?
16. Do you have plans in place for Incident Response, Business Continuity and Disaster Recovery? Yes No
If one or more of these plans are in place, have they been tested? Yes No

MEDIA CONTENT CONTROLS

- 17. Content Review Process – Review Content/Material being disseminated prior to release? Yes No
- 18. Does the Applicant attain proper licensing for Content/Material? Yes No
- 19. Does the Applicant have procedures in place to remove controversial Content/Material? Yes No

CYBER CRIME CONTROLS

- 20. Are all wire transfers subject to a three step process: (a) initiation (b) approval and (c) release? Yes No
If yes, are the steps completed by two or more authorized individuals? Yes No
- 21. Is a callback or alternative notification process in place for all electronic transfers of funds? Yes No
- 22. Do you train your employees concerning the detection of Business Email Compromise (BEC)? Yes No

DECLARATION AND SIGNATURE

During the past five (5) years, has the **Applicant** experienced any incidents, occurrences, **Claims** or **Losses** related to the (i) a **Network Security Breach**, (ii) a **Privacy Violations** or (iii) an **Privacy Threat** or **Security Threat** stemming from the **Applicant** or does the **Applicant** have knowledge of a situation or circumstance which might otherwise result in a **Claim** against the **Applicant** with regard to issues related to the Insurance sought? Yes No
(If 'Yes', please attach complete details.)

Name (Please Print): Title (Must be Principal, Partner, or Officer)

Signature: Date: