YourIT!
Your Logo Goes Here

Cyber Insurance Readiness

Policies and Procedures

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for: Client Company

Prepared by: Your IT Company

Table of Contents

CYBER INSURANCE READINESS Backup and Recovery - Backup and Recovery

CYBER INSURANCE READINESS - Cyber Liability & Theft	**Other Requirements**
Backup and Recovery Backup and Recovery	N/A

Policy
Client Company will implement controls to:

> Backup critical data and systems. Conduct regular test recoveries to ensure that critical functions - not just data and servers - can be restored within the desired RTO.

Purpose
The purpose is to ensure that businesses that purchase cyber insurance meet all the requirements defined in their policies.

Scope
This policy applies to the workforce members and vendors of organizations that come in contact with sensitive, confidential, and/or protected data.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

Related Internal Controls
CYINS-1a - Backup Storage: Backups are stored on premise.
CYINS-1b - Backup Storage: Backups are stored in offline storage.
CYINS-1c - Backup Storage: Backups are stored in offsite storage.
CYINS-1d - Backup Storage: Backups are stored in a secondary data center.
CYINS-6a - Backup Media: The Applicant utilizes tapes for backups.
CYINS-6b - Backup Media: The Applicant utilizes disks for backups.
CYINS-6c - Backup Media: The Applicant utilizes cloud for backups.
CYINS-7a - Backup Protection: Backups are subject to Multi-factor Authentication.
CYINS-7b - Backup Protection: Backups are subject to Encryption.
CYINS-7c - Backup Protection: Backups are subject to Segmentation.
CYINS-7d - Backup Protection: Backups are subject to Virus/malware scanning.
CYINS-7e - Backup Protection: Backups are Immutable.
CYINS-7f - Backup Protection: Backups are subject to Privileged Access Management.

CYINS-8a - Backup Storage: Backups are made to offsite storage every minute.
CYINS-8b - Backup Storage: Backups are made to offsite storage every hour.
CYINS-8c - Backup Storage: Backups are made to offsite storage every day.
CYINS-9a - Backup Storage: Backups are made to offline storage every minute.
CYINS-9b - Backup Storage: Backups are made to offline storage every hour.
CYINS-9c - Backup Storage: Backups are made to offline storage every day.
CYINS-10a - Backup Test: A full recovery from backup is tested every month.
CYINS-10b - Backup Test: A full recovery from backup is tested every calendar quarter.
CYINS-10c - Backup Test: A full recovery from backup is tested every 6 months.
CYINS-10d - Backup Test: A full recovery from backup is tested every year.
CYINS-11 - Backups: The Applicant conducts regular back up of data.

CYBER INSURANCE READINESS Business Continuity - Business Continuity

CYBER INSURANCE READINESS - Cyber Liability & Theft Business Continuity Business Continuity	**Other Requirements** N/A

Policy

Client Company will implement controls to:

> Create written business continuity, disaster recovery, and incident management plans. Include Recovery Time Objectives (RTO) in the plans and test the plans to verify that the RTOs can be met. Implement redundant systems, hot, warm, or cold recovery sites as needed.

Purpose

The purpose is to ensure that businesses that purchase cyber insurance meet all the requirements defined in their policies.

Scope

This policy applies to the workforce members and vendors of organizations that come in contact with sensitive, confidential, and/or protected data.

Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

Related Internal Controls

CYINS-12 - Business Continuity Plan: The applicant has a written Business Continuity Plan.
CYINS-13a - Business Continuity Plan Test: The business continuity plan is tested is tested every month.
CYINS-13b - Business Continuity Plan Test: The business continuity plan is tested is tested every calendar quarter.
CYINS-13c - Business Continuity Plan Test: The business continuity plan is tested is tested every 6 months.
CYINS-13d - Business Continuity Plan Test: The business continuity plan is tested is tested every year.
CYINS-22 - Disaster Recovery Plan: The applicant has a written Disaster Recovery Plan.
CYINS-23a - Disaster Recovery Plan Test: The disaster recovery plan is tested is tested every month.
CYINS-23b - Disaster Recovery Plan Test: The disaster recovery plan is tested is tested every calendar quarter.

CYINS-23c - Disaster Recovery Plan Test: The disaster recovery plan is tested is tested every six months.
CYINS-23d - Disaster Recovery Plan Test: The disaster recovery plan is tested is tested every year.
CYINS-43 - Hot, Warm, Cold Recovery Site: The Applicant maintain a hot, warm or cold site backup IT facility.
CYINS-44a - Incident Response: The expected time to respond to an intrusion is less than one hour.
CYINS-44b - Incident Response: The expected time to respond to an intrusion is 1 hour - 4 hours.
CYINS-44c - Incident Response: The expected time to respond to an intrusion is more than four hours.
CYINS-45 - Incident Response Plan: The applicant has a written Incident Response Plan.
CYINS-46a - Incident Response Plan Test: The incident response plan is tested is tested every month..
CYINS-46b - Incident Response Plan Test: The incident response plan is tested is tested every calendar quarter.
CYINS-46c - Incident Response Plan Test: The incident response plan is tested is tested every six months.
CYINS-46d - Incident Response Plan Test: The incident response plan is tested is tested every year.
CYINS-59 - Manual Workarounds: The Applicant employs a manual workaround in the event of an interruption of the network.
CYINS-89 - Recovery Test: Based upon testing results, it takes 1 - 4 hours to restore the Applicant's critical business operations following a network or systems interruption.
CYINS-90a - Recovery Time Objective - RTO: In the event of an interruption of the Applicant's network, the Applicant's recovery time objective for critical systems, applications and processes is, at most, 1 - 4 hours.
CYINS-90b - Recovery Time Objective - RTO: In the event of an interruption of the Applicant's network, the Applicant's recovery time objective for critical systems, applications and processes is, at most, 4 - 24 hours
CYINS-90c - Recovery Time Objective - RTO: In the event of an interruption of the Applicant's network, the Applicant's recovery time objective for critical systems, applications and processes is, at most, 1 - 2 days.
CYINS-90d - Recovery Time Objective - RTO: In the event of an interruption of the Applicant's network, the Applicant's recovery time objective for critical systems, applications and processes is, at most, more than 2 days.
CYINS-91a - Recovery Time Objective - RTO: The business continuity plan contains recovery time objectives of 1 - 4 hours for the amount of time within which business processes and continuity must be restored.
CYINS-91b - Recovery Time Objective - RTO: The business continuity plan contains recovery time objectives of 4 - 24 hours for the amount of time within which business processes and continuity must be restored.
CYINS-91c - Recovery Time Objective - RTO: The business continuity plan contains recovery time objectives of 1 - 2 days for the amount of time within which business processes and continuity must be restored.
CYINS-91d - Recovery Time Objective - RTO: The business continuity plan contains recovery time objectives of more than 2 days for the amount of time within which business processes and continuity must be restored.
CYINS-92 - Redundant Systems: The Applicant employs redundancy of critical business systems.
CYINS-93 - Redundant Systems: The Applicant is enabled to immediately failover into a redundant information system in the event of an interruption of the network.

CYBER INSURANCE READINESS Compliance - Compliance

CYBER INSURANCE READINESS - Cyber Liability & Theft Compliance Compliance	**Other Requirements** N/A

Policy
Client Company will implement controls to:

Comply with all applicable law, regulations, and contracts.

Purpose
The purpose is to ensure that businesses that purchase cyber insurance meet all the requirements defined in their policies.

Scope
This policy applies to the workforce members and vendors of organizations that come in contact with sensitive, confidential, and/or protected data.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

Related Internal Controls
CYINS-18a - Compliance: The Applicant is currently compliant with, or enabled to demonstrate a defensible compliance position under the European Union General Data Protection Regulation (EU GDPR).
CYINS-18b - Compliance: The Applicant is currently compliant with, or enabled to demonstrate a defensible compliance position under the United Kingdom (UK) General Data Protection Regulation (UK GDPR).
CYINS-18c - Compliance: The Applicant is currently compliant with, or enabled to demonstrate a defensible compliance position under California Consumer Privacy Act (CCPA)/California Privacy Rights and Enforcement Act (CPRA).
CYINS-18d - Compliance: The Applicant is currently compliant with, or enabled to demonstrate a defensible compliance position under Canada's Personal Information Protection and Electronic Data Act (PIPEDA).
CYINS-18e - Compliance: The Applicant is currently compliant with, or enabled to demonstrate a defensible compliance position under the U.S. Biometric Information Privacy Act (BIPA).

CYINS-18f - Compliance: The Applicant is currently compliant with, or enabled to demonstrate a defensible compliance position under the U.S. Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health Act (HITECH).
CYINS-18g - Compliance: The Applicant is currently compliant with, or enabled to demonstrate a defensible compliance position under the U.S. Gramm-Leach-Bliley Act (GLBA).
CYINS-18h - Compliance: The Applicant is currently compliant with, or enabled to demonstrate a defensible compliance position under Fair Credit Reporting Act (FCRA) /Fair and Accurate Credit Transactions Act (FACTA)/Red Flags Rules.
CYINS-18i - Compliance: The Applicant is currently compliant with, or enabled to demonstrate a defensible compliance position under the Telephone Consumer Protection Act (TCPA).
CYINS-18j - Compliance: The Applicant is currently compliant with, or enabled to demonstrate a defensible compliance position under the Controlling the Assault of Non-Solicited Pornography And Marketing Act (CAN-SPAM).
CYINS-18k - Compliance: The Applicant is currently compliant with, or enabled to demonstrate a defensible compliance position under the U.S, Video Privacy Protection Act (VPPA).
CYINS-19 - Compliance: If the Applicant is not compliant with applicable data security standards, please describe the current status of any compliance work and the estimated date of completion.
CYINS-80 - PCI-DSS: The applicant is required to be compliant with PCI-DSS.

CYBER INSURANCE READINESS Data Protection - Data Protection

CYBER INSURANCE READINESS - Cyber Liability & Theft Data Protection Data Protection	**Other Requirements** N/A

Policy
Client Company will implement controls to:

Impement written policies and procedures for:
Access Controls
Advanced Threat Protection
Authentication
Cloud Services
Configuration ManagementEncryption
E-mail Protection
Firewalls
Logging and Log Reviews
Multi-Factor Authentication (MFA)
Network Segmentation
Passwords
Penetration Testing
Personal Device Protection
Third Party Management
Vulnerability Scanning

Purpose
The purpose is to ensure that businesses that purchase cyber insurance meet all the requirements defined in their policies.

Scope
This policy applies to the workforce members and vendors of organizations that come in contact with sensitive, confidential, and/or protected data.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

Related Internal Controls

CYINS-2 - 24x7 Security Operations Center: The Applicant has, or contracts for, a Security Operations Center (SOC) that is monitored 24/7.
CYINS-3 - Access Logs: Access is audited and updated.
CYINS-4 - Administrator Accounts: Changes to administrator accounts are reported automatically.
CYINS-5 - Anti-Virus Software: Up-to-date, active anti-virus software is on all computers, networks, and mobile devices.
CYINS-14 - Centralize Log Storage & Retention: The Applicant has a centralized log collection and management that allows for review of all access and activity on the network.
CYINS-15 - Cloud Service: The Applicant currently uses, or has plans in the next year to use, the services of a cloud service or other outsourced service provider.
CYINS-16a - Cloud Service: An interruption or cessation of cloud services would have no impact on the Applicant’s ability to meet customer contractual obligations.
CYINS-16b - Cloud Service: An interruption or cessation of cloud services would have slight impact on the Applicant’s ability to meet customer contractual obligations.
CYINS-16c - Cloud Service: An interruption or cessation of cloud services would have significant impact on the Applicant’s ability to meet customer contractual obligations.
CYINS-17 - Cloud Service: The Applicant’s disaster recovery or business continuity plan specifically addresses restoration and recovery of business operations provided by a cloud service provider.
CYINS-20 - Configuration Management: The Applicant employs strict security configuration management of personal devices, web applications, servers, databases and critical business and security applications.
CYINS-21a - Critical Patches: Critical updates are implemented within 0 - 60 minutes following release.
CYINS-21b - Critical Patches: Critical updates are implemented within 1 - 24 hours following release.
CYINS-21c - Critical Patches: Critical updates are implemented within 1 - 30 days following release.
CYINS-21d - Critical Patches: Critical updates are implemented within 1 - 12 months following release.
CYINS-24 - DLP: The Applicant employs a data loss prevention solution.
CYINS-25 - EDR: The Applicant employs an endpoint detection and response solution (EDR).
CYINS-26 - EDR: EDR is deployed on all of the Applicant’s endpoints.
CYINS-27 - EDR: EDR is deployed on all of the Applicant’s servers.
CYINS-28a - E-mail Security: The Applicant employs SPF.
CYINS-28b - E-mail Security: The Applicant employs DKIM.
CYINS-28c - E-mail Security: The Applicant employs DMARC.
CYINS-29 - Employee Screening: Job applicants are subject to screening including credit history, criminal records, drug testing as permitted by law.
CYINS-30 - Encryption at Third Parties: The Applicant employs mandatory encryption to protect data while in the care, custody, and control of a third party service provider.
CYINS-31 - Encryption of Data at Rest: The Applicant employs mandatory encryption to protect Personal Information at rest.