<Member Entity>

Technology Policy

Version 1.0

CYBER JIF

NJ CYBER RISK MANAGEMENT FUND

Cybersecurity Framework

Minimum Security Group

1.1 Asset Management

Requirements:

1. Inventory your technology ecosystem: Workstations, end-user devices, network devices, servers, etc.
2. Inventory your technology ecosystem: Software: Operating systems and applications
3. Maintain network diagram.
4. Segment employee Wi-Fi from customer/public Wi-Fi.

1.2 Data Management

Requirements:

1. Create data management process that addresses data sensitivity, owner, retention and disposal.
2. Files with personally identifiable information (PII), protected health information (PHI) and other sensitive/confidential information are password protected or encrypted while being stored and shared.
3. Adhere to any additional cybersecurity practices required by applicable laws or regulations.
4. Inventory your data: Focus on Personally Identifiable Information (PII), Private Health Information (PHI) and other confidential information (police records, video, etc.).
5. Weekly, off-network, off-premises full backup of all data.

1.3 Account Management

Requirements:

1. Maintain inventory of accounts:
    a. Users;
    b. Administrator / Elevated privileges;
    c. Service accounts; and
    d. Shared accounts.
2. Separate administrative/elevated privilege accounts from user accounts and restrict privileges (such as web browsing and email).
3. Must adopt a password policy that at least meets the following Classic Password Policy or meets the NIST Password Standards 800-63B (03/02/2020 Updates), and as further updated.
4. Utilize a Virtual Private Network (VPN) and Multi Factor Authentication (MFA) for all remote connections to your network.
5. Require MFA when accessing cloud-based applications (where capable).
6. Disable or delete accounts that are dormant or inactive for 45 days.
7. Users with administrator rights are limited to those who need them.
8. Non-administrator users are granted limited rights based on job function and responsibility.
9. Access rights are updated upon any personnel status change action.
10. Access rights for each individual are reviewed at least every six (6) months.

Classic Password Policy:

1. **Change Frequency**: Passwords are updated every three (3) months.
2. **Construction**:
    a. Unique from passwords used on all other programs, websites, devices, etc., both personal and work.
    b. Minimum of ten (10) characters.
    c. Sequential or repetitive characters of more than two in succession are not to be permitted. Example: “123”, “AAA”, etc.
    d. Commonly used passwords are not to be permitted. Example, “password”, “123456789”, “qwerty”, “abc123”, etc. Full lists of commonly used passwords can be found in various cybersecurity reports.
    e. Context-specific words are not to be permitted. Example, the name of the application or website being logged into.

3. **Previously Breached Passwords**: The member shall implement a process for identifying breaches containing user email addresses and utilize a breach corpus search for breached passwords, and such passwords shall be updated and not used again.
4. **Failed Login Lockout**: The account shall be locked out after five (5) failed attempts for a period of no less than 30 minutes. In lieu of a timed lockout, the member may utilize a positive identification process to unlock the account.

NIST 800-63B:

1. **Failed Login Lockout**: Limit the number of failed authentication attempts
2. **Password**:
   a. Suggest users use "memorized secrets" instead of passwords
   b. Memorized Secrets are secret values intended to be chosen and memorized by the user; something you know
3. **Length**: 8 characters minimum to at least 64 characters maximum
4. **Change**: Only change if there is evidence of compromise
5. **Screening**: Screen passwords against a list of known compromised passwords
6. **Hints**: Disable password hints and knowledge-based security questions
7. **Composition Minimums**: Skip character composition rules
8. **Composition Restrictions**: Do not allow:
   a. Dictionary words
   b. Repetitive or sequential characters
   c. Context-specific words (i.e. service name or username)
9. **Copy & Paste**: Allow copying and pasting passwords from a password manager
10. **Other Characters**: Allow ASCII and UNICODE, including emojis

1.4 Vulnerability Management

Requirements:

1. Adopt a practice of installing all security and critical updates and patches as soon as practicable based on risk and operational impact, but no longer than a month for high and critical vulnerabilities as defined by CVSS.
   a. For high and critical vulnerabilities that cannot be patched in a month, create an exception process that documents the vulnerability and plan to remediate or otherwise compensate the risk.
2. Keep all operating software, application software and infrastructure equipment current with latest versions.
3. Annually review all non-standard applications for replacement/upgrade.
4. Scan your ecosystem with a vulnerability management tool on a monthly or more frequent basis.

1.5 Defensive Tools & Strategies

Requirements:

1. Microsoft Office applications open all downloaded files in "Protected Mode".
2. Antivirus enabled for all desktops and laptops / servers.
3. Firewalls enabled for all desktops and laptops / servers.
4. Antispam and antivirus filters enabled for the mail server.
5. Firewall rules and policies need to be reviewed or reassessed at least twice per year.
6. Disable autorun for all removable media.
7. Virus scan any removeable media before permitting connection.
8. Disable unused ports.
9. Utilize endpoint detection and response (EDR) tool across entire network.
10. Ensure there are no default accounts or passwords on any organization devices.

1.6 Cyber Hygiene

Requirements:

1. All computer, network or email users receive annual training of at least one hour, including these topics, with such training including phishing exercises:
   a. Malware Identification;
   b. Password construction;

    c. Identifying and responding to security incidents; and
    d. Social engineering attacks.
2. Leadership briefed annually on state of security for the organization, including high impact incidents (breach/loss of PII, funds fraud, intrusion, etc.).
3. Register with Multi-State Information Sharing & Analysis Center (MS-ISAC) and New Jersey Cybersecurity Communication and Integration Cell (NJCCIC). If a Utility Authority, register with your respective ISAC, such as Water ISAC.

1.7 3rd Party Risk Management

Requirements:

1. Maintain an inventory of third-party providers.
2. High Risk Vendors only (IT, Health, PII/PHI):
    a. Ensure contracts include security requirements, indemnification, and proper insurance.
    b. Utilize a 3rd Party Risk Assessment Tool for new/renewing contracts.

1.8 Policies & Procedures

Requirements:

1. Management adopts a cybersecurity incident response plan to direct staff and guide technology management decision making when a cybersecurity incident takes place, which must include at a minimum the items in the Cyber JIF's Cybersecurity Incident Response Plan.
2. Management adopts a Technology Practices Policy, which must include at a minimum each of the subject items outlined in the Cyber JIF's Cyber Risk Management Program.
3. Establish procedures requiring multiple approvals for requests to change banking information.
4. Establish procedures requiring multiple approvals and source verification for financial transaction requests over a certain threshold.

Advanced Security Group

2.1 Asset Management

Requirements:

1. Servers are physically protected from unauthorized access and environmental hazards.
2. Maintain ability to generate asset inventory on demand.
3. Use active discovery tool, including MDM that can install and updated programs on demand.
4. Address unauthorized devices.
5. Maintain ability to generate software inventory on demand.
6. Use an automated inventory tool, whitelist authorized software.
7. Address unauthorized software.
8. Segment your network, separating key units, such as Finance, Human Resources, Police, Utilities, etc.

2.2 Data Management

Requirements:

1. Enforce data management process and ensure proper classification, retention, and disposable.
2. Encrypt all data on removable media.
3. Deploy a data loss prevention tool. Move rarely- and un-unused data off the live network to off-network or segmented storage. Use of standardized system images or virtualized desktops.
4. Deploy a data loss prevention tool.
5. Move rarely-/un-used data off of the live network to off-network or segmented storage.
6. Use of standardized system images or virtualized desktops.
7. Application, Operating System and Network Configuration Software: Back-up copy of current versions must always be available with a copy stored off-premises.
8. Locally stored data:
    a. Daily incremental backups with minimum of 14 days of versioning on off-network device.
    b. All backups are spot-checked monthly.
9. Cloud-Based Applications and Data: Must meet the same standards as the Locally Stored Data.
10. Third-Party Application Data: Vendor must meet the same standards as the Locally Stored Data.

2.3 Account Management

Requirements:

1. Must be able to generate inventory on demand.
2. Use an enterprise password management solution.
3. Use specialized PAM tool.
4. Periodically test all email addresses with an email breach service to determine if any emails have been compromised and take necessary action to ensure integrity.

2.4 Vulnerability Management

Requirements:

1. Use automatic updating where practicable, particularly as related to security patches.

2.5 Logging

Requirements:

1. Logging must be setup for entire network/all devices, such as System, Application and Security logs.
2. Spot check logs monthly.
3. Centralize log collection and build detections off collected logs.

2.6 Defensive Tools & Strategies

Requirements:

1. Ensure only fully supported plug-ins for browsers and email clients are in use.
2. Deploy protective DNS for the ecosystem.
3. Use anti-exploitation and behavior-based anti-malware tools.
4. 24x7 support by phone or email in case of incident.
5. Maintain automated robust alerting and reporting that can prompt human interdiction on a 24x7 basis.

2.7 Cyber Hygiene

Requirements:

1. Administrators and privileged users receive specialized training.
2. Organization leadership has access to expertise that supports technology decision making (i.e., risk assessment, planning, and budgeting).

2.8 3rd Party Risk Management

Requirements:

1. For all vendors, ensure contracts include security requirements, indemnification and proper insurance.
2. For all vendors, utilize a 3rd Party Risk Assessment Tool for all contracts.
3. Risk rank third party providers based on accesses and service provided.
4. Use monitoring solution with continuous monitoring and assessment of third party (high risk).

2.9 Policies & Procedures

Requirements:

1. Develop a Business Continuity Plan for everything technology related.

2.10 Penetration Testing

Requirements:

1. Perform Penetration Testing on an annual basis.