Cyber Risk Management Program

Version 1

9/15/2021

OVERVIEW

The New Jersey Counties Excess Joint Insurance Fund (NJCE) provides its members with cyber insurance coverage. The NJCE has embarked on creating a cyber risk management framework to assist members in managing this evolving risk through the development of a set of minimum technology proficiency standards. The NJCE established a Cyber Task Force to deploy cyber education, release a cyber risk management framework and monitor the cyber risk of its members. The task force is comprised of commissioners, risk managers, executive directors and other professionals.

The NJCE recognizes that much of the terminology and technical aspects of the minimum standards might not make sense to everyone; therefore, it is critical this program be reviewed and enacted on with the assistance of your technology expert. Your technology expert should guide your officials in determining what your organization needs to do to comply.

Keep in mind, these minimum standards will not eliminate all technology risks. The standards are only minimums, which will provide a strong level of protection if effectively carried out; however, cyber risks constantly evolve. This means you must constantly monitor your cybersecurity posture so your organization can respond to new threats and risks as warranted.

GETTING STARTED

1. GET A TECHNOLOGY EXPERT!
2. Review the Cyber Risk Management Program with your technology expert.

   Develop a plan, timetable and budget to implement the standards.

   - *The standards are logically sorted based on importance, effectiveness, cost and complexity.*
3. Complete the Certification checklist initially and continually update as new measures are implemented.
4. Establish a process to at least annually review your technology risks, score how the organization is managing them and ensure the program continues to be met.

Phase	Subject	Requirements	Comments
1	**Information Backup**	1. Use of standardized system images or virtualized desktops 2. Application, Operating System and Network Configuration Software: Back-up copy of current versions must always be available with a copy stored off-premises 3. Locally Stored Data (including MS 365, Google Workspace and similar): a. Daily incremental backups with minimum of 14 days of versioning on off-network device. b. Weekly, off-network, off-premises full backup of all data. c. All backups are spot-checked monthly. 4. Cloud-Based Applications and Data: Must meet the same standards as the Locally Stored Data. 5. Third-Party Application Data: Vendor must meet the same standards as the Locally Stored Data.	1. No comment. 2. Back-up such software or have current installation files available. 3. Backup all locally stored data to local, cloud or off-network devices. MS 365/Google cloud-based and locally stored files require a separate local or cloud-based backup. As this applies to all non-application software, consider cloud storage data. 4. Includes Azure, Google Cloud, AWS, etc. Cloud service application and data files must be backed-up using appropriate cloud services. 5. Obtain in writing the backup practices used by application vendors, and ensure they meet these practices or provide equivalent protection. Consider utilizing FedRamp certified service providers/products.
1	**Patch Management**	1. Keep all operating software, application software and infrastructure equipment current with latest versions. 2. Use automatic updating where practicable, particularly as related to security patches. 3. Install all security and critical updates and patches as soon as prudent and practicable following release. 4. Annually review all non-standard applications for possible replacement/upgrade.	1. No comment 2. No comment 3. System administrators need to coordinate patch upgrades with applications residing on systems managed by third parties to ensure upgrades will not disable their applications. Consider a procedure for these upgrades/patches when Technology Manager may not be available (i.e. vacation). 4. Outdated or non-supported operating systems and software should not be used unless there is no practical alternative available, in which case appropriate steps must be taken to mitigate potential security threats. Please note, patches are not a guarantee solution as they may ultimately have their own security flaws, but they at least fix known issues.
1	**Defensive Software**	1. Antivirus, firewalls, antimalware and antispam enabled for all endpoints and devices, as appropriate (desktops, laptops, mail server, network servers, other ports, etc.) 2. Unused ports closed	1. Should have automatic updates. Microsoft Windows comes with a preloaded firewall. All network servers must have antimalware software running with automatic updates. 2. No comment

		3. Firewall rules and policies need to be reviewed or reassessed at least twice per year 4. Microsoft Office applications open all downloaded files in "Protected Mode" 5. Inventory all devices and endpoints, and review at least twice per year	3. No comment 4. No comment 5. No comment
1	**Endpoint Detection and Response**	1. Deploy endpoint detection tools on all endpoints, addressing data search and investigations, suspicious activity detection, and data exploration. 2. Ensure the detection database is continually monitored and a proper team is available to respond. 3. Deploy endpoint response tools on all endpoints.	1. No Comment 2. No comment 3. Consider Filtering, Advanced Threat Blocking, Threat Hunting and Incident Response, and Multiple Threat Protection.
1	**Security Awareness Training**	All computer users receive annual training of at least one hour. Training includes, but is not limited to: 1. Malware Identification 2. Password construction 3. Identifying and responding to security incidents 4. Social engineering attacks	An expert should perform the training in either virtual or in-person format, which includes the various online training services. Best practice (although not required) is to perform training each quarter. Phishing testing is highly recommended twice per year. You may want to work with your counsel on an employee policy whereby access is removed or other actions taken for not completing/failing the training
1	**Password**	Must adopt a Technology Password Policy that at least meets the standards set in the NJCE's Password Policy, at a minimum, or meet the NIST Password Standards 800-63B (03/02/2020 Updates).	NIST: https://pages.nist.gov/800-63-3/sp800-63b.html
1	**Email Warning**	Add a clear and obvious automatic warning label to all emails coming from outside of your organization.	No comment
1	**Cyber Incident Response Plan**	Management/Governing Body 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 NJCE Cybersecurity Incident Response Plan.	See the NJCE's template Incident Response Plan. The Plan should be annually reviewed, TESTED and updated.
1	**Technology Practices Policy**	Management/Governing Body adopts a Technology Practices Policy, which must include at a minimum each of the subject items outlined in the NJCE Cyber Risk Management Program.	See the NJCE's Technology Practices Policy template. The Policy should be annually reviewed and updated.
1	**Government Cyber Memberships**	1. Register with New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) 2. Register with Multi-State Information Sharing & Analysis Center (MS-ISAC)	1. IT'S FREE! 2. ALSO FREE! If you are/have a utility authority/department, also register for your respective ISAC, such as ICS-CERT (industrial controls), Water-ISAC (water/wastewater) or E-ISAC (electric).

Phase	Subject	Requirements	Comments
2	**Servers**	Servers are physically protected from unauthorized access	Access-controlled rooms, locked cages, etc.
2	**Access Privilege Controls**	1. Users with administrator rights are limited to those who need them 2. Non-administrator users are granted limited rights based on job function and responsibility 3. Access rights are updated upon any personnel status change action 4. Access rights for each individual and job title/function are reviewed at least every six (6) months	1. No comment 2. No Comment 3. This should be added to your personnel action form and routed to technology management 4. No comment
2	**Technology Support**	Staff or contractors are readily available for technology guidance	For vendors, a contract needs to be in place. It does not suffice the organization has the ability to call someone.
2	**Logging**	Logging must be setup for entire network/all devices, such as System, Application and Security logs.	Consider utilizing log-monitoring tools.
2	**Protected Information**	Files with personally identifiable information (PII) and protected health information (PHI) are password protected or encrypted	No comment
2	**Remote Access**	1. Utilize a Virtual Private Network (VPN) for all remote connections. 2. Enable MFA for login to the organization's network, organization's email service (if cloud-based) and with third-party applications passing/storing Protected Information. 3. Adopt a Remote Access practice policy, which must at a minimum include the items in the NJCE's Remote Access Policy.	This is only applicable if you allow remote access to your network (i.e. employees, vendors, etc.). Also consider limiting remote network access to only pre-approved devices with a Network Access Control (NAC). See the NJCE's template Remote Access Policy. Annually review and update the Policy.
2	**Leadership Expertise**	Organization leadership has access to expertise that supports technology decision making (i.e., risk assessment, planning, and budgeting)	This can be any combination of officials, employees, contractors/consultants or citizen volunteers
2	**Technology Business Continuity Plan**	Update your organization's Emergency Management/Continuity of Government (CoG) plan to include digital assets and technology management.	Address most items in your CoG in the Technology Practices Policy. Periodically perform tabletop exercises to ensure effective and efficient disaster response.
2	**Banking Controls**	Implement internal controls and controls with your bank: 1. Establish procedures requiring multiple approvals for requests to change banking information. 2. Establish procedures requiring multiple approvals and source verification for financial transaction requests over a certain threshold.	Ensure compliance with NJDLGS Electronic Payroll and EFT/P-Card rules. 1. No comment 2. Consider setting a low amount, such as $5,000
2	**Technology Practices**	Adopt a Technology Practices Policy, which must include at a minimum each of the subject items in the NJCE Cyber Risk Management Program.	See the NJCE's template Technology Practices Policy. Annually review and update the Policy.

Phase	Subject	Requirements	Comments
3	**Network Segmentation**	Network segmentation.	Consider separating business units, but especially critical/sensitive units, such as finance, police and utilities. Utilities should consider an air-gap for their Industrial Control (ICS) / SCADA systems. Virtual and/or physical segmentation is acceptable.
3	**Logging**	Spot-check logs on at least a monthly basis.	Logs should be spot-checked for accuracy and usability.
3	**Password Integrity**	Periodically test all email addresses against HaveIBeenPwned or a similar email breach service to determine if any emails have been compromised, and take necessary action to ensure integrity.	MS-ISAC, NJCCIC and some vendors may be able to provide this testing.
3	**Third Party Risk Management**	Utilize a 3rd Party Cybersecurity Risk Assessment Tool for new/renewing contracts.	This is most applicable to certain vendors transmitting/storing confidential data, such as technology provider, payroll, HR, etc. Many nationally/internationally recognized certifications suffice, such as SOC2.

<Member Entity>

Technology Policy

Version 1

NJCE Cyber Risk Management Program

Table of Contents

It is essential to review these policies with a qualified and experienced Technology professional to ensure proper understanding and implementation.

1. Policy Statement

The Technology Policy defines the technology security practices necessary to ensure the security of the member's technology systems and the information it stores, processes, and/or transmits.

2. Reason for the Policy

We act as the custodian of a wealth of sensitive information relating to the services we provide and the constituents we serve. We also rely on technology for much of our daily operations. Accordingly, an appropriate set of security measures must be implemented to guard against unauthorized access to, alteration, disclosure, or destruction of this information and/or the technology systems that store, process, or transmit the information.

This policy affirms our commitment to technology security by specifying the policies and standards necessary to achieve our security objectives, including compliance with all Federal and State requirements, as well as the New Jersey Counties Excess Joint Insurance Fund's (NJCE) Minimum Technology Proficiency Standards.

3. Scope

All technology systems and users are expected to comply with this policy.

4. Phase 1 Policies

The member shall implement practices and policies that meet or exceed the NJCE's requirements at a minimum.

4.1. Information Backup Policy

Objective:

The objective of the Information Backup Policy is to ensure all data is regularly backed up and available when needed in the event of an incident (e.g., ransomware, flood, fire, etc.). If the network is virtual, meaning no local data is stored on devices, the requirement to backup devices does not apply.

Requirements:

a) Use of standardized system images or virtualized desktops
b) A back-up of applications, operating systems and network configuration software must always be available
c) Daily incremental backups with a minimum of 14 days of versioning on off-network device of all data
d) Weekly, off-network, full back-up of all data
e) All backups are spot-checked monthly
f) Third-party and cloud-based application data must also be backed-up to the same standards

4.2. Patch Management Policy

Objective:

The objective of the Patch Management Policy is to ensure all systems and applications are patched on a timely basis. Outdated and/or unsupported operating systems/applications shall not be used.

Requirements:

Patch all operating systems, applications, and infrastructure equipment with latest versions.

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

b) All security and critical updates and patches are installed as soon as possible following release. Following are examples:

- Microsoft products (Windows, Desktops, Servers, Office, SQL Data Bases, Outlook, etc.)
- Search engines (Google, Firefox, Microsoft Edge, Bing, etc.)
- Technical infrastructure equipment that requires regular security updates (switches, firewalls, routers, etc.)
- Third-Party applications (finance, animal license, construction, code enforcement, etc.)

c) Annually review all non-standard applications for possible replacement/upgrade

4.3. Defensive Software Policy

Objective:

The objective of the Defensive Software Policy is to ensure all systems are protected by software that minimizes the likelihood of an attack by malicious individuals and/or malware that can compromise the confidentiality, integrity and availability of that system or information.

Requirements:

a) Antivirus, firewalls, antimalware and antispam enabled for all endpoints and devices, as appropriate (desktops, laptops, mail server, network servers, other ports, etc.)
b) Unused ports closed
c) Firewall rules and policies need to be reviewed or reassessed at least twice per year
d) Microsoft Office applications open all downloaded files in “Protected Mode”
e) Inventory all devices and endpoints, and review at least twice per year

4.4. Endpoint Detection and Response

Objective:

The objective of the Endpoint Detection and Response Policy is to ensure we have real-time awareness of potential and actual threats at all endpoints and can effectively respond to such threats to minimize or fully prevent serious incidents.

Requirements:

a) Deploy endpoint detection tools on all endpoints, addressing data search and investigations, suspicious activity detection, and data exploration.
b) Ensure the detection database is continually monitored and a proper team is available to respond.

c) Deploy endpoint response tools on all endpoints.

4.5. Security Awareness Training Policy

Objective:

The objective of the Security Awareness Training Policy is to ensure all personnel with access to the member's technology assets receive appropriate cyber awareness education to reduce the likelihood of a cyber incident by understanding potential cyber threats.

Requirements:

All personnel with access to the member's technology assets shall receive annual training of at least one hour that includes malware identification (email and websites), password construction, identifying security incidents, and social engineering.

4.6. Password Policy

Objective:

The objective of the Password Policy is to ensure that users construct passwords that minimize the likelihood of unauthorized access to the member's data and technology systems.

Requirements:

There are two options for compliance: 1) Follow the set of standards below; or 2) Follow the NIST Password Standards 800-63B (03/02/2020 Updates).

Option 1

1- **Change Frequency**
   a. Network users' passwords are updated every three (3) months.
2- **Construction**
   b. Passwords must be unique from passwords used on all other programs, websites, devices, etc., both personal and work.
   c. Passwords must be a minimum of ten (10) characters.
   d. Sequential or repetitive characters of more than two in succession are not to be permitted.
      - Example: "123", "AAA", etc.
   e. 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.
   f. 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 user 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.

Option 2 (NIST)

1- **Failed Login Lockout**
   a. 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**
   a. 8 characters minimum to at least 64 characters maximum
4- **Change**
   a. Only change if there is evidence of compromise
5- **Screening**
   a. Screen passwords against a list of known compromised passwords
6- **Hints**
   a. Disable password hints and knowledge-based security questions
7- **Composition Minimums**
   a. Skip character composition rules
8- **Composition Restrictions**
   a. Do not allow
      i. Dictionary words
      ii. Repetitive or sequential characters
      iii. Context-specific words (i.e. service name or username)
9- **Copy & Paste**
   a. Allow copying and pasting passwords from a password manager
10- **Other Characters**
   a. Allow ASCII and UNICODE, including emojis

4.7. Email Warning Policy

Objective:

The objective of the Email Warning Policy is to reduce spoofing emails and social engineering emails by identifying when emails are coming from outside the organization.

Requirements:

Example of email warning label:

CAUTION:

This email originated from outside of our email domain. Do not click on links or open attachments unless you recognize the sender and know the content is safe. If unsure, do not reply to this email and call the sender directly.

4.8. Cyber Incident Response Plan

Objective:

The objective of the Incident Response Plan is to define the methods for identifying, tracking, and responding to technology security incidents.

Requirements:

Please refer to the NJCE's Incident Response Plan, attached.

4.9. Technology Practice Policy

Objective:

The objective of the Technology Practice Policy is to ensure management/governing bodies adopt a Technology Practices Policy that includes all the subject items outlined in the NJCE Cyber Risk Management Program.

Requirements:

This document shall serve as the Technology Practice Policy.

4.10. Government Cybersecurity Membership Policy

Objective:

The objective of the Government Cybersecurity Membership policy is to ensure the member stays current with cyber threat notifications and relevant information. Both required below are FREE.

Requirements:

The member shall register and become a member of New Jersey Cybersecurity Communications Integration Cell (NJCCIC) and Multi-State Information Sharing and Analysis Center (MS-ISAC).

New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) - https://www.cyber.nj.gov/

The New Jersey Cybersecurity and Communications Integration Cell is the state's one-stop shop for cybersecurity information sharing, threat intelligence, and incident reporting. Acting in a cyber fusion center capacity, the NJCCIC is a component organization within the New Jersey Office of Homeland Security and Preparedness.

The NJCCIC works to make New Jersey more resilient to cyberattacks by promoting statewide awareness of cyber threats and widespread adoption of best practices. We provide a wide array of cybersecurity services, including the development and distribution of cyber alerts and advisories, cyber tips, and best practices for effectively managing cyber risk. Other services include threat briefings, risk assessments, incident response support, and training.

Multi-State Information Sharing & Analysis Center (MS-ISAC) - https://www.cisecurity.org/ms-isac/

The mission of MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal, and territorial governments through focused cyber threat prevention, protection, response, and recovery.

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation.

We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing technology systems and data. We lead a global community of technology professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

5. Phase 2 Policies

5.1. Server Security Policy

Objective:

The objective of the Server Security Policy is to prevent unauthorized physical access, damage, and interference to the member's server(s) and network equipment.

Requirements:

The member's servers and network equipment shall be protected by physical barriers with restricted access controls and must not be in common public areas. The servers and network equipment may be stored in an enclosed cabinet, data closet, or office with secure entries.

5.2. Access Privilege Controls Policy

Objective:

The objective of the Access Privilege Control Policy is to control access to all technology digital assets. Access to all technology shall be controlled by role-based access controls.

Requirements:

a. System and Network administrative rights are to be limited to those who are authorized to make changes to the systems, computers, and network.
b. Network and system access to file and folders are granted based on the individual's job function and level of responsibility.
c. Access rights need to be reviewed and updated upon any personnel change. Exiting employees' access must be revoked immediately upon separation.
d. A review process is to be implemented to ensure access rights are up to date. Minimal review frequency is six (6) months.

5.3. Technology Support Policy

Objective:

The objective of the Technology Support Policy is to ensure the member has the technical support expertise and structure in place to effectively mitigate and triage technology and cyber related issues.

Requirements:

Technical support can be provided by a qualified and experienced employee or vendor.

5.4. System and Event Logging Policy

Objective:

The objective of the Logging Policy is to ensure system activities, information security events, and system utilization and performance are captured.

Requirements:

The member shall use the following Microsoft logs (or similar for other operating systems) to monitor system activities, information security events, and system utilization and performance.

a) System
b) Application
c) Security

Note: There are numerous free and for-cost log management tools on the market.

5.5. Protected Information Policy

Objective:

The objective of the Protected Information Policy is to ensure all digital files and data containing sensitive information, Personally Identifiable Information (PII), and Protected Health Information (PHI) are protected in accordance with statutory, regulatory, and contractual requirements.

Requirements:

All digital documents containing Personally Identifiable Information (PII), Protected Health Information (PHI) and documents deemed by the member as sensitive shall be encrypted.

5.6. Remote Access Policy

Objective:

The purpose of Remote Access Policy is to secure remote access connectivity into the member's network using a Virtual Private Network (VPN) and Multi-Factor Authentication (MFA).

Requirements:

The member shall deploy a Virtual Private Network (VPN) for those who need to remotely access the member's network. Only approved users, third-parties, vendors, and contractors may utilize the VPN service

to connect to the member's network. VPN profiles shall be created upon request from the relevant department head, approving authorities, or designated sponsor. Multi Factor Authentication (MFA) shall be enabled for login to the organization's network, email service (if cloud-based) and third-party applications passing/storing Protected Information.

The following Remote Security Controls shall be enabled for devices remotely accessing the above connections:

- The member shall require employees to immediately report a lost or stolen device.
- The member shall maintain the ability to remotely wipe a user's member-owned device.

The member shall maintain the ability to disconnect any user from the member's network.

Using Personal Devices:

The following requirements only apply to those approved users, third-party, vendor or contractors who use their personal devices to access the member's network.

- All personal devices must be up to date with all applicable operating systems, security patches and virus/malware protection software.
- Users with remote access privileges shall ensure their remote access connection is used explicitly for member work and used in a manner consistent with their on-site connection to the member's network.
- Personal equipment shall not be used to connect to the member network unless authorized and approved in writing by someone in senior management charged with approving cybersecurity changes.
- VPN users are automatically disconnected from the member network after thirty (30) minutes of inactivity. The user must then logon again to re-authenticate in order to reconnect to the network.
- All personal devices are required to use a password to protect from tampering using the same standards and requirements as the member's equipment.
- The member shall not allow remote users to save any data to their personal devices (i.e. member can utilize Content Access Controls or a Cloud Access Security Broker).

5.7. Leadership Expertise Policy

Objective:

The objective of the Leadership Expertise Policy is to ensure the member's senior management has access to resources with expertise in their respective fields to support technology decision making, such as risk assessments, planning, budgeting, etc.

Requirements:

The member's senior management shall have access to resources with expertise in their respective fields leveraging their technology support and the NJCE's available resources.

5.8. Technology Business Continuity Plan Policy

Objective:

The objective of the Technology Business Continuity Plan Policy is to ensure the member is prepared and can effectively recover from a disruption in service, including cyber breaches, denial of service or ransomware attacks, and be able to restore continuity of operations.

Requirements:

The Emergency Management/Continuity of Government (CoG) plan shall include a Technology Business Continuity Plan as part of its Disaster Recovery section.

When developing a Technology Business Continuity Plan the member shall consider the following:

Recovery Strategies

a) Identify all operational functions
b) Identify key support personnel and communications plan
c) Prioritize based on Recovery Time Objectives (RTOs)
d) Consider and accommodate the following impacts:
    - Loss of Computing (Systems and Data)
    - Loss of Telecommunications
    - Loss of Personnel
    - Denial of Physical Access
    - Critical vendors' services

5.9. Banking Control Policy

Objective:

The objective of the Banking Control Policy is to prevent or reduce fraudulent banking transactions.

Requirements:

The member shall implement internal controls to minimize fraudulent banking transactions. The following are required:

- Use Multi-Factor Authentication when accessing the bank's system and making financial transactions, where available.
- Establish procedures requiring multiple approvals for request to change banking information.
- Establish procedures requiring multiple approvals and source verification for financial transaction requests over $5,000.

6. Phase 3 Policies

6.1. Network Segmentation Policy

Objective:

The objective of the Network Segmentation Policy is to reduce the spread of a cyber-attack by dividing the network into multiple zones or sub-networks, virtually or physically, and applying security protocols to each zone. The member shall consider isolating key business units or sensitive departments, such as finance and human resources.

Requirements:

Divide the network into multiple zones or sub-networks, virtually or physically, and apply security protocols to each zone. The member shall consider isolating key business units or sensitive departments, such as finance and human resources.

Utilities shall have an "air gap" between their primary network and their Industrial Control System (ICS) / SCADA system. An air gap is a network security measure that physically isolates one network from another to prevent external connections.

6.2. Password Integrity Policy

Objective:

The objective of the Password Integrity Policy is to frequently validate users' emails and passwords to ensure they have not been compromised.

Requirements:

The member shall implement a process where user emails are checked against an email breach service, such as HaveIBeenPwned, to determine if any email addresses have been compromised. Member must take necessary action to ensure integrity of any emails found to in the breach database.

The HaveIBeenPwned website is: https://haveibeenpwned.com/

6.3. System and Event Logging Policy

Objective:

Logs shall be reviewed every three (3) months by the technology professional.

Requirements:

Logs shall be reviewed every three (3) months by the technology professional.

Note: There are numerous free and for-cost log management tools on the market.

6.4. Third-Party Risk Management Policy

Objective:

The objective of the Third-Party Risk Management (TPRM) Policy and Procedure is to ensure the protection of information that is accessible to outside vendors. It is important to properly identify and manage risks associated when working with third-party vendors.

Requirements:

Vendor Review Process *(New and Existing Vendors)*

A Vendor Review shall take place for those vendors/partnerships who store, handle, access, and/or transmit any of the following sensitive data:

- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Financial information
- Credit card information
- Access to the member's information system and/or computer network
- Any asset deemed sensitive and/or of value

The Vendor Review shall be in the form of an extensive Third-Party Security Questionnaire (attached and embedded below) which shall be forwarded to the vendor for completion. Following receipt of the questionnaire and any requested supporting documentation, the *Vendor Relationship Manager*** shall engage the appropriate qualified and experienced professionals, including their Risk Manager, to review and opine on the information provided. The overall risk associated with the selection of the vendor shall be carefully considered.

***Vendor Relationship Manager* – Person responsible for the service, product, or agreement being requested.

Technology Vendors

It is paramount to select a technology vendor that has the expertise, experience, and certification to effectively design, implement, manage, and maintain your technology system.

Requirements:

The following is a sample list of items that should be considered:

- Do they have the experience?
- Are they reliable and with references?
- Do they stay current with technology and trends?
- Do they provide a contract with Service Level Agreements (SLA)?
- Do they recommend ways to improve the performance and security of your network?
- Can they recommend how to design your network with security controls in mind?
- Can they design a network with redundancy built in to recover from a major incident?

Technology Support Guidelines

Industry Standard Certifications	Certifications required based on support role					
	Help Desk Support	PC / Printer Repair	Server Repair & Support	System Administration	Network & Infrastructure Support	Information Security
HDI technical support professional certification	✓					
CompTIA IT Fundamentals (ITF+)	✓	✓				
CompTIA A+	✓	✓	✓	✓		
CompTIA Network +			✓	✓	✓	
CompTIA Server +			✓	✓	✓	

CompTIA Security +			●	●	✓	✓
MCSE			●	✓	●	●
CCNA					✓	✓
CISSP						✓
CEH						✓

- Certifications marked with a bullet are not required but good to have depending on customer needs.

CompTIA IT Fundamentals (ITF+)	Entry level certification focusing on essential IT skills and knowledge such as the functions and features of common operating systems, establishing network connectivity, security best practices and how to identify common software applications.
CompTIA A+	The certification focuses on validating nine major IT skills, including hardware, operating systems, software troubleshooting, networking, hardware and network troubleshooting, security, mobile devices, virtualization and cloud computing and operational procedures.
CompTIA Network +	The certification focuses on configuring, managing, and maintaining network devices, implementing, and designing functional networks, network troubleshooting and network security.
CompTIA Server +	The certification focuses on knowledge of server hardware and technology as well as troubleshooting and repairing server issues, including disaster recovery.
CompTIA Security +	The certification focuses on threats, attacks and vulnerabilities, risk management, architecture and design, technology and tools, cryptography and PKI and identity and access management.
MCSE Microsoft Certified Systems Engineer	Though Microsoft has retired the MCSE certification program as of June 30, 2020, the certification focuses on designing, managing, and supporting Windows products and architecture.
CCNA Cisco Certified Network Associate	The CCNA certification focuses network fundamentals, network access, IP connectivity, IP services, security fundamentals and automation and programmability.
CISSP Certified Information Systems Security Professional	The CISSP certification focuses on critical security issues, including risk management, cloud computing, application development security, mobile security, etc.
Certified Ethical Hacker	The CEH certification specializes in penetration testing, vulnerability testing, and cyber forensics analysis.

< Organization >

Cyber Incident Response Plan

Table of Contents

1. Policy Statement

The Incident Response Plan defines our methods for identifying, tracking, and responding to technology-based security incidents.

2. Reason for the Policy

The Incident Response Plan is established to assist in protecting the integrity, availability, and confidentiality of technology and assist in complying with statutory, regulatory and contractual obligations.

Responding quickly and effectively to an Incident is critical to minimizing the spread of the Incident and/or the business, financial, legal, and/or reputational impact. Incident Response generally includes the following phases:

- Detection, Reporting, and Analysis.
- Legal.
- Forensics.
- Containment, Eradication, and Recovery.
- Other Responses (i.e. Public Relations).
- Post-Incident Review.

3. Scope

This plan governs incidents that have a significant negative impact on information technology systems and/or sensitive information (hereinafter, "Incidents"). Incidents can include denial of service, malware, ransomware, and/or phishing attacks that can significantly affect operations and/or result in the unintended disclosure of sensitive data (e.g., constituent data, Protected Health Information, Personally Identifiable Information, credit card data, and law enforcement records).

Minor events (e.g., routine detection and remediation of a virus, a minor infraction of a security policy, or other similar issues that have little impact on day-to-day business operations) are not considered an Incident under this policy.

4. Incident Identification

For cyber insurance purposes, a security incident is an event that is a: cyber security breach, cyber extortion threat, or data breach.

4.1 Cyber Extortion Threat

A threat against a network to:

1. Disrupt operations.
2. Alter, damage, or destroy data stored on the network.
3. Use the network to generate and transmit malware to third parties.
4. Deface the member's website.
5. Access personally identifiable information, protected health information, or confidential business information stored on the network; made by a person or group, whether acting alone,

or in collusion with others, demanding payment, or a series of payments in consideration for the elimination, mitigation, or removal of the threat.

4.2 Cyber Security Breach

Any unauthorized access to, use, or misuse of, modification to the network, and/or denial of network resources by attacks perpetuated through malware, viruses, worms, Trojan horses, spyware, adware, zero-day attack, hacker attack, or denial of service attack.

4.3 Data Breach

The actual or reasonably suspected theft, loss, or unauthorized acquisition of data that has or may compromise the security, confidentiality and/or integrity of personally identifiable information, protected health information, or confidential business information.

Other cyber security incidents include:

- Attempts from unauthorized sources to access systems or data.
- Unplanned disruption to a service or denial of a service.
- Unauthorized processing or storage of data.
- Unauthorized changes to system hardware, access rights, firmware, or software.
- Presence of a malicious application, such as ransomware, or a virus.
- Presence of unexpected/unusual programs.

5. Designation of an Incident Response Manager

The organization shall designate an Incident Response Manager who is either a full or part time technology person working in your organization on a daily basis or the highest-ranking administrative person in your organization that employees would normally contact when having computer or technology problems. Ideally, this person should be readily available to employees in the case of a cyber security event.

5.1 Responsibilities

- The organization has designated an Incident Response Manager that is responsible for determining whether an event, or a series of security events, is declared an Incident.
- The Incident Response Manager is responsible for ensuring that this policy is followed.
- The Incident Response Manager is responsible for establishing an Incident Response Team to support the execution of this plan.
- The Incident Response Team is tasked with executing this plan in accordance with and at the direction of the Incident Response Manager.
- The highest-ranking administrative official in the organization is responsible for ensuring that end-users have sufficient knowledge to recognize a potential security Incident and report it in accordance with this plan.
- Employees are responsible to report potential security incidents in a timely manner and provide any requires support during plan execution.

6. Incident Response Team and Notification

Establish an incident response team to be able to quickly respond to cyber security incidents, and a team broad enough to gather the needed resources and make the appropriate decisions to resolve the incident. Such team shall include the following.

Title / Position	Name	Telephone #
Highest-ranking Administrative Official		
Chief of Police (if applicable)		
General Counsel		
Human Resources Manager		
Incident Response Manager		
JIF Risk Management Consultant		
JIF Claims Administrator		
Technology Support Contact		

Please verify with your breach advisor/counsel that their firm will be handling the required breach notifications including, but potentially not limited to, those agencies listed below.

IC3	FBI Internet Crime Complaint Center: https://www.ic3.gov/
NJ Cybersecurity and Communications Integration Cell (NJCCIC)	Incident Reporting: https://www.cyber.nj.gov/report 609-963-6900 x7865

7. Incident Response Phases

7.1 Detection, Reporting, & Analysis

1. If a user, employee, contractor, or vendor observes a potential security event they should notify the Incident Response Manager immediately. If the Incident Response Manager is not available, the events should be immediately reported to the highest-ranking administrative official.
2. The Incident Response Manager is responsible for communicating the Incident, its severity, and the action plan to the highest-ranking administrative official.
3. If the Incident Response Manager or the highest-ranking administrative official are not available, a user should isolate the affected devices from the network or internet by removing the network cable from the device. If operating via wireless, turn off the wireless connection. If isolating the machine from the network is not possible then unplug the machine from its power source.
4. If you have determined or suspect that the Incident is a cyber security breach, cyber extortion threat, or data breach (*see Definitions Related to Cyber Liability Insurance – Section 4 of this document*) proceed to Step 5. If not, proceed to Step 6.
5. For a cyber security breach, please follow this process:
6. *If the Incident is determined not to be a cyber security breach, cyber extortion threat, or data breach*, the Incident Response Manager should work with the Incident Response Team to assess the Incident, develop a plan to contain the Incident, and ensure the plan is communicated to and approved by the highest-ranking administrative official.

7. The Incident Response Manager should ensure that all actions are documented as they are taken and that the highest-ranking administrative official, Incident Response Team, and outside support are regularly updated.

7.2 Containment, Eradication, & Recovery

Containment is the act of limiting the scope and magnitude of the attack as quickly as possible. Containment has two goals: preventing data of note from being exfiltrated and preventing the attacker from causing further damage.

Immediate triage:

1. Immediately contact technology expert to report the event and follow their instructions. It is now the responsibility of technology expert to notify management of the incident and to execute the security incident response plan.

2. If technology expert is not available, isolate the affected devices from the network or internet by removing the network cable from the device. If operating via wireless, turn off the wireless connection. DO NOT TURN OFF DEVICE OR REMOVE POWER SOURCE unless instructed by technology expert.

3. Incident response team assembles and assesses if the incident is a cyber security breach, cyber extortion threat, or data breach. If it is, or if there is any question the incident may or may not be one, management contacts their JIF Claims Administrator to advise them of the incident and management (or technology support) will call the Cyber Insurer Hotline. Work with the breach coach and the other partners they suggest to help resolve the incident.

4. Document all actions as they are taken.

Eradication is the removal of malicious code, accounts, or inappropriate access. Eradication also includes repairing vulnerabilities that may have been the root cause of the compromise. A complete reinstallation of the OS and applications is preferred.

Recovery allows business processes affected by the Incident to recover and resume operations. It generally includes:

- Reinstall and patch the OS and applications.
- Change all user and system credentials.
- Restore data to the system.
- Return affected systems to an operationally ready state.
- Confirm that the affected systems are functioning normally.

7.3 Forensics

Security incidents of a significant magnitude may require that a forensics investigation take place. Once that need has been established all additional investigation/containment activities need to be directed and/or performed by a forensics specialist to ensure that the evidence and chain of custody is maintained. The highest-ranking administrative official, in consultation with the Incident Response Manager and/or XL Caitlin will advise if engaging a forensics firm is required.

7.4 Post-Incident Review

To improve the Incident Response processes and identify recurring issues each Incident should be reviewed and formally reported on. The report should include:

- Information about the Incident type
- A description of how the Incident was discovered.
- Information about the systems that were affected.
- Information about who was responsible for the system and its data.
- A description of what caused the Incident.
- A description of the response to the Incident and whether it was effective.
- A timeline of events, from detection to Incident closure
- Recommendations to prevent future Incidents.
- A discussion of lessons learned that will improve future responses.

8. Periodic Review

This policy and associated subordinate procedures will be reviewed at least annually by the Incident Response Manager to adjust processes considering new risks and security best practices. Material changes in this policy should be approved by the highest-ranking administrative official and/or governing body of the organization.

9. Special Situations/Exceptions

Any personally owned devices, such as PDAs, phones, wireless devices, or other electronic devices which have been used to access organizational data and are determined to be relevant to an Incident, may be subject to retention until the Incident has been eradicated.