Getting Started!

1. GET A TECHNOLOGY EXPERT!
2. Review the Cyber Risk Management Program with your technology expert.
3. Develop a plan, timetable and budget to implement the standards.
4. Once implemented, complete the Certification checklist.
5. 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.

Tier	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. Images and virtual desktops must be kept current with manufacturer patches. 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.
1	**Defensive Software**	1. Antivirus and firewalls enabled for all desktops and laptops 2. Antispam and antivirus filters enabled for the mail server 3. Firewall enabled on all active ports, unused ports closed, antivirus enabled and antimalware enabled for network servers that connect to the internet 4. Firewall rules and policies need to be reviewed or reassessed at least twice per year 5. Microsoft Office applications open all downloaded files in “Protected Mode”	1. Should have automatic updates. Microsoft Windows comes with a preloaded firewall. 2. No comment 3. All network servers must have antimalware software running with automatic updates. 4. No comment 5. No comment

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 '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 Cybersecurity Incident Response Plan.	See the '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 Cyber Risk Management Program, as respects Tier 1.	See the '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).

Tier	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 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 available for technology guidance	For vendors, a contract needs to be in place. It does not suffice that 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**	Utilize a Virtual Private Network (VPN) for all remote connections.	This is only applicable if you allow remote access to your network (i.e. employees, vendors, etc.).
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 Cyber Risk Management Program, as respects Tier 1 and 2.	See the 's template Technology Practices Policy. Annually review and update the Policy.
2	**Remote Access**	Adopt a Remote Access practice policy, which must at a minimum include the items in the 's Remote Access Policy	

Tier	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	**Remote Access**	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.	This is only applicable if you allow remote access to your network (i.e. employees, vendors, etc.). It is also recommended to limit remote network access to only pre-approved devices with Network Access Control (NAC).
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 the 's 3rd Party 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. You may also consider asking the vendor to become compliant with the 's Cyber Risk Management Program.