Minimum Security

Security Controls	CIS v8 Mapping	Description	Completed
Asset Management	Inventory and Control of Enterprise Assets (CIS 1)	1. Inventory your technology ecosystem: Workstations, end-user devices, network devices, servers, etc.	
	Inventory and Control of Software Assets (CIS 2)	1. Inventory your technology ecosystem: Software: Operating systems and applications	
	Network Infrastructure Management (CIS 12)	1. Maintain network diagram.	
		2. Segment employee Wi-Fi from customer/public Wi-Fi.	
Data Management	Data Protection (CIS 3)	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.).	
	Data Recovery (CIS 11)	1. Weekly, off-network, off-premises full backup of all data.	
Account Management	Account Management (CIS 5)	1. Maintain inventory of accounts: a. Users, b. Administrator / Elevated privileges, c. Service accounts, d. Shared accounts.	
		2. Separate administrative/elevated privilege accounts from user accounts, and restrict privileges (such as web browsing and email).	
	Access Control Management (CIS 6)	1. Must adopt a Technology Password Policy that at least meets the standards set in the attached Password Policy, at a minimum, or meet the NIST Password Standards 800-63B (03/02/2020 Updates), and as further updated.	
		2. Utilize a Virtual Private Network (VPN) and Multi Factor Authentication (MFA) for all remote connections to your network.	
		3. Require MFA when accessing cloud-based applications (where capable).	
		4. Disable or delete accounts that are dormant or inactive for 45 days.	
		5. Users with administrator rights are limited to those who need them.	
		6. Non-administrator users are granted limited rights based on job function and responsibility.	
		7. Access rights are updated upon any personnel status change action.	
		8. Access rights for each individual are reviewed at least every six (6) months.	
Vulnerability Management	Continuous Vulnerability Management (CIS 7)	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.	
		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.	

Minimum Security

Security Controls	CIS v8 Mapping	Description	Completed
Defensive Tools & Strategies	Email and Web Browser Protections (CIS 9)	1. Ensure only fully supported browsers and email clients are in use.	
		2. Add a clear and obvious automatic warning banner to all emails coming from outside of your organization.	
	Malware Defenses (CIS 10)	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.	
	Network Monitoring Defense (CIS 13)	1. Utilize endpoint detection and response (EDR) tool across entire network.	
	Secure Configuration of Enterprise Assets and Software (CIS 4)	1. Ensure there are no default accounts or passwords on any organization devices.	
Cyber Hygiene	Security Awareness and Skills Training (CIS 14)	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 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.	
3rd Party Risk Management	Service Provider Management (CIS 15)	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.	
Policies & Procedures	Incident Response Management (CIS 17)	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 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 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.	

Minimum Security

This document must be signed by the mayor, municipal administrator, or municipal clerk (or director of entity if not a municipality) AND your technology expert.

MEMBER ENTITY

Print Name _____ Title _____

Signature _____ Date _____

TECHNOLOGY EXPERT

Print Name _____ Title _____

Signature _____ Date _____

Advanced Security

Security Controls	CIS v8 Mapping	Description	Completed
Asset Management	Inventory and Control of Enterprise Assets (CIS 1)	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.	
	Inventory and Control of Software Assets (CIS 2)	1. Maintain ability to generate software inventory on demand.	
		2. Use an automated inventory tool, whitelist authorized software.	
		3. Address unauthorized software.	
	Network Infrastructure Management (CIS 12)	1. Segment your network, separating key units, such as Finance, Human Resources, Police, Utilities, etc.	
Data Management	Data Protection (CIS 3)	1. Enforce data management process and ensure proper classification, retention, and disposable	
		2. Encrypt all data on removable media.	
	Data Recovery (CIS 11)	1. Deploy a data loss prevention tool.	
		2. Move rarely-/un-used data off of the live network to off-network or segmented storage.	
		3. Use of standardized system images or virtualized desktops.	
		4. Application, Operating System and Network Configuration Software: Back-up copy of current versions must always be available with a copy stored off-premises.	
		5. 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. All backups are spot-checked monthly.	
		6. Cloud-Based Applications and Data: Must meet the same standards as the Locally Stored Data.	
		7. Third-Party Application Data: Vendor must meet the same standards as the Locally Stored Data.	
Account Management	Account Management (CIS 5)	1. Must be able to generate inventory on demand.	
	Access Control Management (CIS 6)	1. Use an enterprise password management solution.	
		2. Use specialized PAM tool.	
		3. 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.	
Vulnerability Management	Continuous Vulnerability Management (CIS 7)	1. Use automatic updating where practicable, particularly as related to security patches.	
Logging	Audit Log Management (CIS 8)	1. Logging must be setup for entire network/all devices, such as System, Application and Security logs.	
		2. Spot check logs on a monthly basis.	
		3. Centralize log collection and build detections off collected logs.	

Advanced Security

Security Controls	CIS v8 Mapping	Description	Completed
Defensive Tools & Strategies	Email and Web Browser Protections (CIS 9)	1. Ensure only fully supported plug-ins for browsers and email clients are in use.	
		2. Deploy protective DNS for the ecosystem.	
	Malware Defenses (CIS 10)	1. Use anti-exploitation and behavior-based anti-malware tools.	
	Network Monitoring Defense (CIS 13)	1. 24x7 support by phone or email in case of incident.	
		2. Maintain automated robust alerting and reporting that can prompt human interdiction on a 24x7 basis.	
Cyber Hygiene	Security Awareness and Skills Training (CIS 14)	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).	
3rd Party Risk Management	Service Provider Management (CIS 15)	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).	
Policies & Procedures	Incident Response Management (CIS 17)	1. Develop a Business Continuity Plan for everything technology related.	
Penetration Testing	Penetration Testing (CIS 18)	1. Perform Penetration Testing on an annual basis.	

This document must be signed by the mayor, municipal administrator, or municipal clerk (or director of entity if not a municipality) AND your technology expert.

MEMBER ENTITY

Print Name	Title
Signature	Date

TECHNOLOGY EXPERT

Print Name	Title
Signature	Date