Requirements for NYMIR Cyber Insurance

- **Data Backups:** Perform regular data backups to ensure data availability in case of incidents like ransomware attacks or data corruption. Use automated backup solutions, store backups offsite, and maintain backup logs.
- **Secure Data Backups:** Safeguards backup copies from tampering or unauthorized access, ensuring data integrity. Use strong encryption algorithms and prevent unauthorized changes to backup data by having a backup stored off-network or immutable.
- **Backup Testing:** Test backups regularly to verify the recoverability of data backups, reducing downtime in the event of data loss. Perform both full and incremental backup tests at least annually, ensuring data can be restored successfully.
- **Encryption:** Protect sensitive data with strong encryption practices, to safeguard sensitive data from unauthorized access, maintaining data confidentiality. Use encryption algorithms like AES, manage encryption keys securely, and conduct vulnerability scans.
- **Managed Firewall:** Implement a robust firewall to control network traffic to protect against unauthorized access, intrusion attempts, and data breaches by creating a barrier between the internal network and external threats. Regularly update firewall rules, monitor network traffic, and configure intrusion detection.
- **Endpoint Protection:** Secure all municipal devices with antivirus and/or Endpoint Detection and Response (EDR), to defend against a wide range of cyber threats, preventing malware infections and safeguarding sensitive data on municipal devices. Configure real-time scanning, automatic updates, and centralized management.
- **Secured Remote Access (if applicable):** Ensure secure remote access and disable unnecessary network ports, to reduce entry points for attackers, protecting the network from unauthorized access and potential breaches. Implement VPNs for secure remote access, conduct regular port scans, and disable unused ports.
- **Multi-Factor Authentication (MFA):** Enforce MFA for remote access to systems and email and consider it for admin users to add an extra layer of protection by requiring multiple forms of authentication, reducing the risk of unauthorized access. Use authentication apps or hardware tokens.
- **Secured Public Wi-Fi (if applicable):** Enhance public Wi-Fi security with encryption and user authentication to safeguard transmitted data on public Wi-Fi networks, preventing eavesdropping and unauthorized access. Implement WPA3 encryption, use strong authentication methods, and isolate guest networks.

- **Email Security:** Improve email security to mitigate the risk of email-based attacks, such as phishing and malware distribution, protecting sensitive data. Train employees to recognize phishing emails, use email encryption for sensitive information, and configure robust spam filters.
- **Complex Passwords:** Enforce strong passwords or passphrases to mitigate password-related risks, making it harder for attackers to guess or crack passwords. Although a minimum of 8 characters is mandatory, it's advisable to opt for longer passwords of at least 12 characters, incorporating a mix of uppercase, lowercase, numbers, and special characters for enhanced security.
- **Access/Account Management:** Implement proper access control and conduct regular access privilege reviews, to prevent unauthorized access to critical systems and data. Use role-based access control, revoke unnecessary permissions, and conduct periodic reviews.
- **Personal Mobile Phone Protection:** Extend security measures to personal mobile devices, reducing the risk of mobile-related security incidents. Implement MFA on mobile devices, enforce access control policies, and provide mobile security guidelines.
- **Updated & Patched Software:** Regularly update all software to protect against known vulnerabilities and exploits, reducing the risk of software-related breaches. Implement automated patch management and schedule vulnerability scans.
- **Employee Training:** Offer employee cybersecurity training at least annually to enhance employees' ability to recognize and respond to cyber threats, reducing the likelihood of falling victim to attacks. Provide security awareness training and phishing prevention programs, which are FREE services available to you if you have NYMIR cyber coverage.
- **Incident Response Plan:** Develop a comprehensive Incident Response Plan outlining the steps to be taken in the event of a cybersecurity incident. Assign roles and responsibilities, create communication protocols, and establish a clear incident escalation process. NYMIR has an Incident Response template that can be adapted to the needs of your municipality.
- **EFT Policy & Secondary Verification:** Establish EFT policies and practices to prevents fraudulent electronic funds transfers and ensure financial security. Implement verification processes for new requests or changes to existing information, secondary authorization for financial transactions, and establish clear EFT guidelines.
- **Compliant with Security Standards:** Ensure compliance with Payment Card Industry Data Security Standard (PCI DSS) requirements, which include securing payment card data, implementing access controls, and regularly assessing and testing security systems.