Municipal Cybersecurity: New York's Chapter 177 Mandate

Robert Braumuller, Esq
Zaina Khoury, Esq.

This page intentionally left blank

Data Security Laws Applicable to New York Municipalities and Public Authorities

A Legal Primer

Presented by Robert Braumuller, Esq. and Zaina Khoury, Esq.

May 18, 2026

BLEAKLEY PLATT
ATTORNEYS AT LAW

914.949.2700
Fax: 914.683.6956
WWW.BPSLAW.COM
One North Lexington Avenue
White Plains, New York 10601

Data Security Requirements

Generally Applicable Data Security Laws:

- New York municipalities are regulated under multiple cybersecurity statutes depending on the municipality's functions and the type of data that they possess.

  - **Chapter 177 of the Laws of 2024 created a new Article 19-C of the General Municipal Law and amended parts of the State Technology Law:** Article 19-C imposes a new cybersecurity program mandate on Municipal Corporations and Public Authorities.

  - **NYS SHIELD Act:** The SHIELD Act requires entities to maintain reasonable safeguards to protect private information and to comply with the statute's breach notification requirements.

  - **FOIL / record retention laws**: These laws affect how municipalities manage, preserve, and disclose information.

Data Security Requirements *(Continued)*

- **Additional Laws Governing Specific Types of Data (health, education, law enforcement, payments, tax):**

  - HIPAA/HITECH Act - provides for the security of protected health information through administrative, physical, and technical safeguards. Applies when entity operates health services, such as, ambulance service.

  - Family Educational Rights and Privacy Act (FERPA) - requirements to safeguard student education records.

  - NYS Education Law § 2-d - mandates a Parents' Bill of Rights, data security standards, and strict contracts with third-party vendors to safeguard personally identifiable information of students, principals, and teachers.

  - FBI's Criminal Justice Information Services (CJIS) - regulations to ensure security of sensitive criminal justice data applicable when entity has a police force.

  - IRS Federal Tax Information Rules - require secure handling of tax returns and return information received from the IRS.

  - PCI DSS (Payment Card Industry Data Security Standard) – mandatory security standards for any entity handling branded credit/debit cards.

GML Article 19-C Cyber Security

Municipal Corporation:

- Under the General Municipal Law (GML), a “municipal corporation” includes a county, city, town, village, fire district, and school district. GML § 119-n.

- For Chapter 177 training rule, State Technology Law § 103-f also reaches a “district” as defined in GML § 119-n.

Public Authority:

- ‘Public authority’ shall mean any public authority or public benefit corporation created by or existing under this chapter or any other law of the state of New York, at least one of whose members is appointed by the governor or another state officer or body, or which is a subsidiary of such a public authority or public benefit corporation. GML § 995-a.

GML Article 19-C

On June 26, 2025, Governor Kathy Hochul signed into law Chapter 177 of 2025 (S.7672A / A.6769A), a new cybersecurity law aimed at enhancing the cybersecurity and resilience of state and local government networks across New York. Effective January 1, 2026, all municipal corporations and public authorities in New York must comply with new requirements around cyber incident reporting, ransomware transparency, employee training, and data protection.

SUMMARY

Article 19-C requires municipal corporations and public authorities to:

- report cybersecurity incidents and demands of ransom payments to the Division of Homeland Security and Emergency Services;
- conduct cybersecurity incident reviews;
- ensure employees undergo cybersecurity awareness training;
- and implement policies to comply with cybersecurity protection and data protection standards for state-maintained information systems.

1. CYBERSECURITY INCIDENT REPORTING (72 HOURS)

- All municipalities and public authorities must report cybersecurity incidents to the New York State Division of Homeland Security and Emergency Services (DHSES) within 72 hours of detection. GML § 995-b (2).

- "Cybersecurity incident" means an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infra-structure controlled by computers or information systems, or information resident thereon. GML § 995-a.

2. RANSOM PAYMENT REPORTING (24 HOURS + 30 DAYS)

- If a ransom payment is made in connection with a ransomware attack, it must be reported within 24 hours of the transaction. GML § 995-c.

- Within 30 days of a ransom payment, the entity must submit a detailed report outlining the:

    - amount paid and method of payment;
    - the rationale behind the decision;
    - alternative options considered; and
    - all diligence performed to ensure compliance with state and federal regulations; such as, the US Department of the Treasury Office of Foreign Assets Control (OFAC) guidelines.

- "Ransomware attack" is defined as an incident that includes the use or threat of use of unauthorized or malicious code or digital disruption used to extort payment. GML § 995-a.

3. Confidentiality of Reports

- Incident reports and ransom disclosures submitted to DHSES are exempt from Freedom of Information Law (FOIL) requests, encouraging transparency without fear of public exposure. GML § 995-b (3).

- DHSES will assess all reported incidents for threats to public health, safety, and security. The agency may coordinate with state and federal law enforcement to share intelligence and offer technical support.

4. Annual Cybersecurity Awareness Training (NYS Technology Law § 103-f)

- All state, county, city, town, village, and district employees who use technology as part of their job duties must complete annual cybersecurity training starting in 2026.

- Training will be overseen and made available by the Office of Information Technology Services (ITS). ITS provides free training videos for New York State and municipal employees. See: https://its.ny.gov/local-government-information-and-cybersecurity-awareness-training. However, this training requirement may be satisfied by the completion of another cybersecurity awareness training.

- All training shall be conducted during regular paid work hours. The law does not mandate a minimum number of hours but requires employees to participate in training once each year.

5. CYBERSECURITY STANDARDS

- GML Article 19-C introduces data protection and cybersecurity standards for public information systems managed by the state. Local governments are encouraged, but not required, to align with these standards to improve preparedness.

- Municipalities should nonetheless adopt these standards and implement reasonable administrative, technical, and physical safeguards for data security to comply with the NYS SHIELD Act. Local governments should adhere to the security and notification standards set by the NYS Technology Law § 208 and the NYS SHIELD Act.

NYS Technology Law § 208

New York State Technology Law § 208, enacted in 2005, established a breach notification framework that applies specifically to "state entities" The statute defines "state entity" to mean "any state board, bureau, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for the state of New York," expressly excluding "all cities, counties, municipalities, villages, towns, and other local agencies"

Rather than leaving municipalities without any data breach obligations, however, § 208 imposes a specific requirement: any entity excluded under this provision (i.e., municipalities and other local agencies) "shall adopt a notification policy no more than one hundred twenty days after the effective date of this section. Such entity may develop a notification policy which is consistent with this section or alternatively shall adopt a local law which is consistent with this section"

§ 208. Notification; person without valid authorization has acquired private information

§ 899-aa. Notification; person without valid authorization has acquired private information

THE NYS SHIELD ACT

The Stop Hacks and Improve Electronic Data Security Act (NYS SHIELD Act) applies to any person or business that holds computerized private information of New York residents and imposes more data security requirements on entities that collect such information. N.Y. Gen. Bus. Law § 899-aa and § 899-bb. It is unclear if the SHIELD Act applies to municipalities but we recommend acting as if it does because it set out clear standards and arguably establishes best practices.

- **"Private Information"** is defined as either:
    i. Personal information (any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person) in combination with any one or more of the following data elements: (i) social security number; (ii) driver's license number or non-driver identification card number; (iii) account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account; (iv) account, credit, or debit card numbers where such number could be used without other identifying information, security code, access code, or password to access an individual's financial account, (v) biometric information, such as fingerprints, voice prints, and retina or iris images, that are used to authenticate or ascertain an individual's identity, (vi) medical information, and (vii) health insurance information, or

    i. A username or e-mail address in combination with a password or security question and answer that would permit access to an online account.

The SHIELD Act has two prongs: (1) the reasonable security requirement and (2) the data breach notification requirement.

I. Reasonable Security Requirement

- The NYS SHIELD Act requires entities to adopt safeguards to protect the security, confidentiality, and integrity of private information. Entities should implement a security program, employee training, vendor contract risk assessments, and timely and secure data disposal. Additionally, the SHIELD Act requires organizations to designate an employee to oversee cyber-security operations.

- The SHIELD Act generally does not mandate specific safeguards. Rather, it provides several examples of practices that are considered reasonable administrative, technical and physical safeguards.

Administrative Safeguards:

- Designate individual(s) responsible for security programs;
- Conduct a risk assessment process that identifies reasonably foreseeable internal and external risks and assesses the sufficiency of safeguards in place to control those risks;
- Train and manage employees in security program practices and procedures;
- Select capable service providers and require safeguards by contract;
- Adjust program(s) in light of business changes or new circumstances.

Physical Safeguards:

- Assess security risks of information storage and disposal;
- Adopt written policies and practices to detect, prevent, and respond to intrusions;
- Protect against unauthorized access/use of private information during or after collection, transportation, and destruction/disposal; and
- Securely dispose of private information within a reasonable amount of time after it is no longer needed for business purposes.

Technical Safeguards:

- Assess risks in network and software design;
- Assess risks in information processing, transmission, and storage;
- Detect, prevent, and respond to attacks or system failures; and
- Regularly test and monitor the effectiveness of key controls, systems, and procedures.

II. SHIELD Act's Data Breach Notification Requirements

The law requires that the person or business notify the affected residents after discovering a breach in the security of its computer data system affecting private information. The disclosure must be made in the most expedient time possible consistent with legitimate needs of law enforcement agencies (with a strict 30-day deadline for notifying individuals and agencies). The law requires notice to the Office of the New York State Attorney General (OAG), the New York Department of State, and the New York State Police of the timing, content, and distribution of the notices and approximate number of affected persons. However, submission of a breach form through the OAG's data-breach-reporting portal is sufficient, as the information is automatically sent to all agencies.

Penalties for violations of the SHIELD Act

Under the SHIELD Act, the Attorney General may seek injunctive relief, restitution, and penalties against any business entity for violating the law.

- For failure to provide timely notification, the court may impose a civil penalty of up to $20 per instance of failed notification, not to exceed $250,000.

- For failure to maintain reasonable safeguards, the court may impose a civil penalty of up to $5,000 per violation.

Enforcement against Municipalities

Article 19-C is structured as a mandatory reporting requirement rather than a penal statute. The Primary "Enforcement" Mechanism is through audits by the Office of the State Comptroller (OSC). Between 2019 and late 2023, the OSC released over 190 IT audits of local governments and school districts, identifying more than 2,400 cybersecurity-related issues. Failure to remediate identified security deficiencies can impact a municipality's credit rating, insurance eligibility, and eligibility for, or success in, state funding applications.

The NY Attorney General (AG) has exclusive enforcement authority for the SHIELD Act. To date, however, the AG has focused primarily on private corporations (e.g., banks, retailers), rather than fining municipalities. We found no report of New York State fining a town or village for poor data security.

PRACTICAL CONSIDERATIONS

New York municipalities and public authorities should:

- Develop and maintain a Data Security Compliance Program with written policies and procedures. Include breach-notification playbooks by data type.
- Develop or revise internal cyber incident and ransomware response protocols and reporting workflows.
- Ensure all employees receive annual training by assigning training responsibility and implementing protocols to track compliance.
- Budget for the legal and operational resources necessary to fulfill reporting obligations.
- Maintain adequate cyber liability insurance coverage.
- Assess which systems qualify as covered information systems and evaluate digital exposure of such infrastructure and systems.

PRACTICAL CONSIDERATIONS (*Continued)*

- Develop a process to coordinate effectively with state and federal partners. Coordinate IT, clerk/records, counsel, HR, police, and communications.

- Ensure all contracts with vendors and contractors have necessary data protection language, cybersecurity provisions, and breach notification obligations and require adequate cyber insurance to meet these strict data protection standards and breach reporting requirements.

- Deploy encryption and data loss prevention tools. Use Multi-Factor Authentication (MFA), logging, backups, vulnerability management.