LOCAL GOVERNMENT MANAGEMENT GUIDE

Information Technology Governance Security Self-Assessment

Office of the New York
STATE COMPTROLLER
Thomas P. DiNapoli

Local Government and
School Accountability

INFORMATION TECHNOLOGY SERIES

Security Self-Assessment

Information Technology Governance

Security Self-Assessment

⚠ ***CAUTION:*** *Upon completion, this document will likely contain content that is confidential or otherwise sensitive in nature and should be handled accordingly.* ⚠

The Information Technology Governance LGMG can downloaded at

www.osc.ny.gov/files/local-government/publications/pdf/information-technology-governance.pdf

This form is available for download and completion online at

https://www.osc.ny.gov/files/local-government/publications/pdf/IT-Governance-Self-Assessment-Form.pdf

Date completed:

IT Policy

1a. Are IT policies adopted, distributed and updated as necessary?

YES☐ NO☐ N/A☐

List policies, their (physical or electronic) locations and the dates adopted and last revised:

1b. Was a breach notification policy adopted? YES☐ NO☐ N/A☐

Date adopted:

Date last revised:

1c. Was a data security and privacy policy adopted? YES☐ NO☐ N/A☐

Date adopted:

Date last revised:

IT Security Training and Awareness

2a. Were all computer users provided IT security training?

YES☐ NO☐ N/A☐

Date(s) of training:

Who attended the training?

2b. Have all officers and employees with access to personally identifiable information (PII), and specifically in schools, those with access to student, teacher or principal PII, been provided with data privacy and security awareness training within the past year?

YES☐ NO☐ N/A☐

Date(s) of training:

Who attended the training?

2c. Are there other efforts to raise IT security awareness?

YES☐ NO☐ N/A☐

Describe awareness efforts:

Computer Hardware, Software and Data Inventories

3a. Is a detailed, up-to-date inventory of computer hardware maintained?

YES☐ NO☐ N/A☐

Review a copy of the hardware inventory and note when last updated:

3b. Is a detailed, up-to-date inventory of authorized software maintained?

YES☐ NO☐ N/A☐

Review a copy of the software inventory and note when last updated:

3c. Has data been assigned to categories (data classification) that will help determine the appropriate level of controls?

YES ☐ NO ☐ N/A ☐

Review a copy of the data classification, noting the categories and types of information in each:

3d. Is a detailed, up-to-date inventory of data maintained?

YES ☐ NO ☐ N/A ☐

Review a copy of the data inventory and note when last updated:

Contracts and Service Level Agreements for IT Services

4a. Do contracts and SLAs for IT services specify the level of service to be provided by the vendor and specific remedies if those requirements are not met?

YES ☐ NO ☐ N/A ☐

Review the contract(s) and note the date signed:

4b. Does any contract that involves sharing student, teacher or principal PII with the third-party contractor include all required elements?

YES ☐ NO ☐ N/A ☐

Confidentiality requirement:

Bill of rights supplement:

Contractor's data security and privacy plan:

Malware Protection

5a. Is antivirus software up-to-date on all computers? YES ☐ NO ☐ N/A ☐

Describe the process for updating antivirus software:

Date of last antivirus software update:

5b. Are removable devices, such as USB flash drives and digital cameras, automatically scanned for viruses and other malware when connected to a local government or school computer?

YES☐ NO☐ N/A☐

5c. Is the AutoPlay feature turned off (e.g., in network security settings) for all removable devices?

YES☐ NO☐ N/A☐

Patch Management

6a. Are operating system and other software programs maintained at vendor-supported versions and are patches and updates applied and installed in a timely manner?

YES☐ NO☐ N/A☐

Describe the process for upgrading an operating system or other software program when it is no longer supported by the vendor:

Describe the process for identifying, applying and installing relevant software patches and updates:

Access Controls

7a. Are unique network user accounts created for each user?

YES☐ NO☐ N/A☐

7b. Are unique application user accounts created for each user where applicable?

YES☐ NO☐ N/A☐

7c. Do any accounts exist that cannot be tied to an authorized user or process?

YES☐ NO☐ N/A☐

Describe the process for disabling unneeded user accounts:

7d. Is a current list of authorized users and their levels of access maintained and periodically reviewed?

YES☐ NO☐ N/A☐

Review the list of authorized users and their levels of access:

7e. Have password expectations been established for administrators configuring passwords or users creating passwords?

YES☐ NO☐ N/A☐

Describe expectations and how those expectations are communicated:

7f. Have password requirements been defined related to for example, password comparisons, invalid attempts or encryption?

YES☐ NO☐ N/A☐

Identify the requirements and describe how each is enforced:

Online Banking

8a. Do you have an online banking policy? YES☐ NO☐ N/A☐

Review the policy:

8b. Are online banking duties properly segregated? YES☐ NO☐ N/A☐

Who has access to prepare, approve, process and record transactions for each online bank account?

8c. Are online bank accounts monitored? YES☐ NO☐ N/A☐

Who monitors the accounts?

How often are online accounts monitored?

Wireless Network

9a. Are wireless access points set up to limit broadcasting from beyond your offices?

YES ☐ NO ☐ N/A ☐

Where are the wireless access points located?

How far does the wireless signal broadcast?

9b. Has the service set identifier (SSID or name of the wireless network) been changed from the factory default?

YES ☐ NO ☐ N/A ☐

What is/are the SSID(s)?

9c. Is the most secure encryption available used? YES ☐ NO ☐ N/A ☐

Note type of encryption used:

Firewalls and Intrusion Detection

10a. Is a firewall(s) in place to control network communications?

YES ☐ NO ☐ N/A ☐

Who is responsible for maintaining firewall rules and settings?

10b. Are firewall activities/events logged? YES ☐ NO ☐ N/A ☐

Who reviews the logs?

10c. Has intrusion detection been automated using modern antivirus software, a firewall(s) or a dedicated intrusion detection system (IDS)?

YES ☐ NO ☐ N/A ☐

Who is responsible for reviewing and investigating any unauthorized, unusual or sensitive access activity identified?

What process is followed to determine whether any security violation constitutes a breach requiring notification of affected individuals?

Physical Controls

11a. Is physical access to IT system resources including servers, computers, network devices and wiring closets (if any) restricted?

YES ☐ NO ☐ N/A ☐

View the server, computer, network device and wiring closet areas/rooms. How is access granted to those areas/rooms (e.g., key, security code, access card)?

11b. Are areas with IT system resources including servers, computers, network devices and wiring closets protected from fire and water damage?

YES ☐ NO ☐ N/A ☐

11c. Is there an uninterrupted power source? YES ☐ NO ☐ N/A ☐

11d. Are inspections conducted for physical security control weaknesses?

YES ☐ NO ☐ N/A ☐

Who conducted the last inspection and on what date?

Information Technology Contingency Planning

12a. Has an IT contingency plan been developed? YES ☐ NO ☐ N/A ☐

Review the plan and note the date adopted:

12b. Has the plan been distributed to responsible parties?

YES ☐ NO ☐ N/A ☐

12c. When was the last time the plan was tested?

What was the outcome of the testing?

12d. Is the plan periodically reviewed and revised as necessary to ensure it still meets local government or school needs?

YES ☐ NO ☐ N/A ☐

Date plan last revised:

12e. Are all critical data files and software programs periodically backed up?

YES ☐ NO ☐ N/A ☐

How often are backups performed?

Date/time of last backup:

Date data was last restored successfully from a backup:

12f. Are backups stored offline and offsite? YES ☐ NO ☐ N/A ☐

How are backups protected against the electronic threats (e.g., cyberattacks such as ransomware) to which the original is exposed?

Where is the offsite storage and how is it secured?

⚠ **CAUTION:** Upon completion, this document will likely contain content that is confidential or otherwise sensitive in nature and should be handled accordingly. ⚠

The Information Technology Governance LGMG can downloaded at
www.osc.ny.gov/files/local-government/publications/pdf/information-technology-governance.pdf

This form is available for download and completion online at
https://www.osc.ny.gov/files/local-government/publications/pdf/IT-Governance-Self-Assessment-Form.pdf

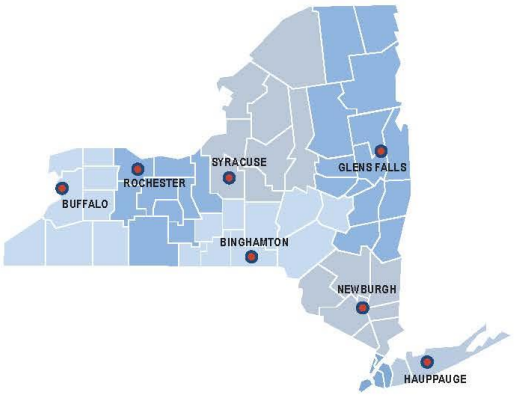
Contacts

New York State Comptroller
THOMAS P. DiNAPOLI

Division of Local Government and School Accountability

110 State Street, 12th Floor, Albany, NY 12236
Tel: 518.474.4037 • Fax: 518.486.6479
Email: localgov@osc.ny.gov

www.osc.ny.gov/local-government



Andrea C. Miller
Executive Deputy Comptroller

Executive • 518.474.4037
Robin L. Lois, CPA, Deputy Comptroller
Randy Partridge, Assistant Comptroller

Audits, Local Government Services and Professional Standards • 518.474.5404
(Audits, Technical Assistance, Accounting and Audit Standards)

Local Government and School Accountability Help Line • 866.321.8503 or 518.408.4934
(Electronic Filing, Financial Reporting, Justice Courts, Training)

Division of Legal Services
Municipal Law Section • 518.474.5586

New York State & Local Retirement System
Retirement Information Services
Inquiries on Employee Benefits and Programs
518.474.7736

Technical Assistance is available at any of our Regional Offices

BINGHAMTON REGIONAL OFFICE
Tel 607.721.8306 • **Fax** 607.721.8313 • **Email** Muni-Binghamton@osc.ny.gov
Counties: Broome, Chemung, Chenango, Cortland, Delaware, Otsego, Schoharie, Tioga, Tompkins

BUFFALO REGIONAL OFFICE
Tel 716.847.3647 • **Fax** 716.847.3643 • **Email** Muni-Buffalo@osc.ny.gov
Counties: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming

GLENS FALLS REGIONAL OFFICE
Tel 518.793.0057 • **Fax** 518.793.5797 • **Email** Muni-GlensFalls@osc.ny.gov
Counties: Albany, Clinton, Columbia, Essex, Franklin, Fulton, Greene, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington

HAUPPAUGE REGIONAL OFFICE
Tel 631.952.6534 • **Fax** 631.952.6530 • **Email** Muni-Hauppauge@osc.ny.gov
Counties: Nassau, Suffolk

NEWBURGH REGIONAL OFFICE
Tel 845.567.0858 • **Fax** 845.567.0080 • **Email** Muni-Newburgh@osc.ny.gov
Counties: Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester

ROCHESTER REGIONAL OFFICE
Tel 585.454.2460 • **Fax** 585.454.3545 • **Email** Muni-Rochester@osc.ny.gov
Counties: Cayuga, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates

SYRACUSE REGIONAL OFFICE
Tel 315.428.4192 • **Fax** 315.426.2119 • **Email** Muni-Syracuse@osc.ny.gov
Counties: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence

STATEWIDE AUDIT
Tel 716.847.3647 • **Fax** 716.847.3643 • **Email** Muni-Statewide@osc.ny.gov

APPLIED TECHNOLOGY UNIT
Tel 518.738.2639 • **Fax** 518.486.6479 • **Email** Muni-Cyber@osc.ny.gov

osc.ny.gov

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability

110 State Street, 12th floor
Albany, New York 12236

Tel: (518) 474-4037
Fax: (518) 486-6479
or email us: localgov@osc.ny.gov

www.osc.ny.gov/local-government

FOLLOW US: osc.ny.gov/subscribe