Office of the NEW YORK STATE

COMPTROLLER

Local Government Management Guide

Information Technology Governance

New York State Comptroller

THOMAS P. DiNAPOLI

DECEMBER 2021

Table of Contents

Information Technology Governance

Many local governments and schools invest a considerable amount of resources into their information technology (IT) systems including, but not limited to, costs for computers and related hardware equipment, software, Internet access, cybersecurity and personnel training. They rely on IT systems for storing and processing important financial and nonfinancial information, accessing the Internet, communicating through email and reporting to State and federal agencies. These systems and the data they hold are valuable and need to be protected from unauthorized, inappropriate and wasteful use. Protecting IT assets is especially important given the ongoing and increasingly sophisticated threat of ransomware[1] attacks against local governments and schools.

Although no single practice or policy on its own can adequately safeguard your IT investments, there are a number of internal controls that, if appropriately implemented and monitored, collectively increase the odds that your systems and data will remain safe. Management, including the governing board, is responsible for ensuring that the right IT internal controls are in place and performing as intended. This can be a challenging task, given the rapid pace of technological innovation, the ever-increasing sophistication and number of cybersecurity threats, and the fact that IT is integral in nearly all aspects of local government and school operations.

Although no single practice or policy on its own can adequately safeguard your IT investments, there are a number of internal controls that, if appropriately implemented and monitored, collectively increase the odds that your systems and data will remain safe.

The following guidance is intended to make oversight less daunting by providing a path for understanding and strengthening IT internal controls. It includes a Security Self-Assessment structured around 12 key areas of IT security that is intended to help you exercise effective IT operation oversight. This serves as a starting point for discussions with personnel who are responsible for the day-to-day management of your IT operations. Because the assessment is geared toward small- to medium-sized computing environment operations, we limited the number of questions. In many cases, there are more questions you could and possibly should ask to fully evaluate and monitor your IT internal controls.

Responsibility for IT Internal Controls

Internal controls are essential to the effective operation of local governments and schools. They encompass the policies, procedures and activities designed to provide reasonable assurance that operations are functioning as intended. In general, properly designed and implemented controls reduce the likelihood that significant errors or fraud will occur and remain undetected. Internal controls over IT seek to ensure that computer systems and the data they process, transmit and store can be trusted; are available when needed; and are adequately protected from unauthorized access and use.

The governing board's internal control responsibilities primarily involve authorization, oversight and ethical leadership. Generally, governing boards do not design internal controls or develop the written policies they adopt. The governing board instead, relies upon management, primarily the chief executive officer (CEO), to create the policies needed to ensure that operations are performed effectively and assets are safeguarded. The CEO in turn relies upon managers and department heads to recommend and implement procedures to help inform staff how to achieve objectives set forth in policies. Some local governments and schools use an IT vendor for assistance in establishing, conducting and monitoring IT internal controls.

An important way that governing boards fulfill their oversight responsibilities is by asking questions related to controls over IT systems and any key applications (e.g., financial, personnel and student information) within those systems. Depending on how IT responsibilities are assigned, the governing board's questions might be directed to the CEO, IT manager, department head(s) or an IT vendor. Asking the right questions is not only an effective way to exercise oversight, it can be done at little or no cost. On the other hand, not asking the right questions may potentially expose IT systems and data to loss or unauthorized access and use, which could be very expensive.

> …[A] background in IT is not necessary to ask questions about key IT internal controls and understand the answers.

It is understandable that someone with little or no IT knowledge might be apprehensive about asking questions concerning IT internal controls. However, a governing board has responsibility for the oversight of the organization's IT operations – whether or not its members are knowledgeable about or feel comfortable discussing IT. As you will note after reviewing the IT Governance Security Self-Assessment included at the end of this document, a background in IT is not necessary to ask questions about key IT internal controls and understand the answers. Extensive IT knowledge is also not necessary to perform certain procedures (e.g., review documents or reports) that can corroborate the answers to the self-assessment questions and help you better understand the condition of the internal controls' effectiveness.

IT Security Fundamentals

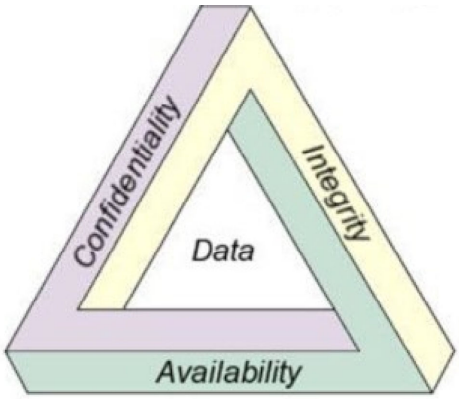
Prior to examining your organization's IT internal controls, it is important to understand two concepts that are fundamental to how IT professionals approach data, network and system security: the CIA triad and defense-in-depth. These concepts highlight the importance of looking at internal controls both individually and collectively and will help you place the internal controls in context.

CIA Triad

The CIA triad refers to an information security model comprised of three main components: confidentiality, integrity and availability. Each component represents a fundamental objective of information security. The CIA triad is a well-known model in information security development. It is applied in various situations to identify problems or weaknesses and to establish security solutions. The model is an industry standard with which most IT professionals should be familiar.

> …[C]onfidentiality, integrity and availability. Each component represents a fundamental objective of information security.

- **Confidentiality** is closely linked with privacy and relates to preventing or minimizing unauthorized access to and disclosure of data and information. To ensure confidentiality, information must be organized in terms of who ought to have access to it as well as its sensitivity.



- **Integrity** is focused on ensuring that data is not tampered with during or after submission. Having accurate and complete data is essential for good decision-making. What good is the information if it cannot be trusted?

- **Availability** means that the information is available when it is needed. Data that cannot be accessed will prove to be of little value. The most available systems are accessible at all times and have safeguards against software or system errors, hardware failures, power outages, natural disasters, and attempts by individuals with malicious intent to cause disruption.

Defense-in-Depth

Defense-in-depth refers to the implementation of multiple layers of security to protect data, networks and IT systems. Building successive layers of defense mechanisms can reduce the risk of a successful attack by someone with malicious intent and is considered a best practice by IT security professionals. A combination of controls helps ensure that your system does not become overly dependent on any one control or layer of security and provides added protection in case a layer of security fails to function properly or does not prevent or stop a threat to your data or system. There is no single control that can be used to adequately protect against today's sophisticated threats. Only a combination of multiple preventive, detective and responsive internal controls will help keep your data and systems safe.

Information Technology Governance: Security Self-Assessment

The Security Self-Assessment at the end of this document addresses key areas of IT internal controls such as policy, training, access and contingency planning. Several of the main questions include follow-up questions that will elicit information helpful for evaluating the answers. For example, one of the questions is, “Were all computer users provided IT security training?” The question is followed by a prompt to record the date(s) of training and who attended, if applicable. If all computer users were provided with IT security training but that training occurred six years ago, the governing board may want to consider arranging for additional training or a refresher in the near future. Likewise, if only a small handful of computer users have received IT security training, the governing board should be aware of that as well.

Some questions are followed by a suggested step you can take to verify and better understand the answer provided. For example, if an up-to-date list of computer equipment is maintained, you could obtain a copy of the inventory listing and review it for reasonableness (i.e., does the inventory make sense given what you know about the local government or school and its operations). This would help you assess whether the list is truly up-to-date. For example, if the inventory of computer equipment does not include any laptop computers, yet you have observed staff working on laptop computers, you may want to ask a follow-up question about the apparent omission from the records.

Because computing environments and operations change over the course of time, governing boards should periodically review IT controls. We recommend that this be done at least once a year.

Similarly, when completing the access controls section of the assessment, you could review a current list of authorized computer users and their levels of access. If names on the list are unrecognizable or if the list contains individuals no longer employed by the local government or school, you could ask appropriate follow-up questions. In addition, questions about access to particular software applications may arise. For example, a member of the governing board may notice that someone with no accounting responsibilities has access to the local government or school’s accounting program.

The following guidance will help you to understand each internal control on the Security Self-Assessment and why it is important to the security and oversight of your IT systems. It should be noted that the manner in which the answers to the questions are obtained is up to the governing board. Board members could interview appropriate responsible parties such as the IT manager or IT vendor (if applicable) in person and ask follow-up questions or obtain additional information for clarification purposes at that time. Alternatively, the governing board could give the self-assessment to the appropriate responsible parties and ask that they complete and return it. In any event, the governing board will probably need to speak with IT personnel and other key staff who play critical roles in the IT internal control environment to ask additional questions, obtain more details regarding the answers provided and discuss the next steps to be taken. Because computing environments and operations change over the course of time, governing boards should periodically review IT controls. We recommend that this be done at least once a year.

IT Security: Key 12 Areas of Concern

Area #1 – IT Policy

IT policies define the Board's expectations for appropriate user behavior, describe the tools and procedures used to help protect data and IT systems, assign key responsibilities and explain the consequences of policy violations. The governing board should provide oversight and leadership by adopting IT policies that take into account people, processes and technology; communicating the policies to all computer users; and ensuring there are procedures in place to monitor compliance with policies.

Your unique computing environment should dictate the content and number of policies necessary. A small entity with uncomplicated, modest computing resources may only need a few policies to cover relevant issues adequately. Larger entities with complex systems may need several policies to convey management's expectations and ensure effective operation. While IT policies will not guarantee the safety of your IT system, a lack of appropriate policies significantly increases the risk that data, hardware and software systems may be lost, damaged or compromised by unauthorized or inappropriate access and use.

At a minimum, IT policies should include:

- **Breach Notification** – New York State Technology Law (State Technology Law) requires municipalities and other local agencies to have a breach notification policy or local law.[2] Such policy or local law must require that notification be given to certain individuals when there is a breach of the security of the system as it relates to private information. If you fail to adopt an information breach notification policy and private information is compromised, or is reasonably believed to be compromised, officials and employees may not understand or be prepared to fulfill their legal obligation to notify affected individuals.

While IT policies will not guarantee the safety of your IT system, a lack of appropriate policies significantly increases the risk that data, hardware and software systems may be lost, damaged or compromised by unauthorized or inappropriate access and use.

- **Data Security and Privacy** – New York State Education Law (State Education Law) and the Commissioner's Regulations (Regulations) require educational agencies to have a data security and privacy policy that aligns with the National Institute for Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.[3] Such policy must also address the data privacy protections in Section 2-d of the State Education Law, including requiring that every use and disclosure of student, teacher or principal[4] personally identifiable information (PII) benefits the student, teacher or principal and prohibiting student, teacher or principal PII from being included in public reports or other documents. [5]

- **Online Banking** – Before a local government or school begins processing financial transactions online, it should have a comprehensive policy that addresses online banking activities. The policy should identify what online banking activities are allowed; who is authorized to prepare, approve and process online transactions; who is responsible for recording online transactions; who is responsible for reviewing and reconciling transactions and how often such reviews and reconciliations should occur; and what procedures should be followed when responding to potential fraudulent activity.

- **Internet, Email, and Computer Use** – This policy should describe what constitutes appropriate and inappropriate use of IT resources, along with your expectations concerning personal use of IT equipment and user privacy (e.g., management reserves the right to examine email, personal file directories, web access history and other information stored on local government or school computers, at any time and without notice). It should also describe the consequences for policy violations (e.g., an employee found to have violated the policy may be subject to disciplinary action, up to and including termination of employment).

Other key topics that you should consider covering in IT policies include but are not limited to:

- **Password Security** – This should address password length, complexity and age requirements, and the number of consecutive failed log-on attempts the system will allow.

- **Mobile Devices** – This should identify any mobile devices[6] explicitly authorized or prohibited from containing or accessing your information resources. It should define the devices covered (e.g., local government or school owned or personally owned), procedures for reporting lost or stolen devices, the process used for gaining approval before connecting new devices to the system and other user responsibilities.

- **Wireless Security** – This should specify whether or not users are allowed to connect local government or school devices to public wireless networks (e.g., at hotels or cafes) and personally owned devices to the local government's or school wireless network. If public wireless network access is allowed, any required security controls, such as virtual private network connections, should be clearly defined. It should also indicate who is covered by the policy (e.g., all employees, contractors, consultants, temporary and other workers) and describe the consequences of violating the policy.

Area #2 – IT Security Training and Awareness

A well-informed workforce is essential to securing electronic data and IT systems. Local governments and schools cannot protect the confidentiality, integrity and availability of their data and systems without ensuring that the people who use and manage IT understand IT security policies and procedures and their roles and responsibilities related to IT security. While the IT policies provide guidance to computer users as to what the governing board expects them to do, IT security training provides them with the skills to do it.

Educational agencies are required to annually provide data privacy and security awareness training to their officers and employees with access to student, teacher or principal PII.[7] The training must cover the federal and State laws governing confidentiality of student, teacher or principal PII, and how employees can comply with those laws.

There have been many accounts of users whose actions caused significant IT system harm or financial losses. They may have been fooled, via social engineering scams,[8] into providing their passwords, opening harmful attachments or visiting malicious websites. Even system administrators, who are typically regarded as having advanced IT knowledge, have been tricked into performing actions that threatened or caused harm to their systems. The success of social engineering, coupled with the never-ending flow of new and innovative threats, underscores the importance of including all users in IT security training. It is also important to update the training material periodically to address new technologies, threats and any changes to your computing environment.

IT security training should explain the proper rules of behavior for using your IT systems and data, and communicate the policies and procedures that need to be followed.

IT security training should explain the proper rules of behavior for using your IT systems and data, and communicate the policies and procedures that need to be followed. The content of training programs should be directed at the specific audience (e.g., user or system administrator) and include everything related to IT security that attendees need to know to perform their jobs. IT security awareness efforts should reinforce your IT policies and training and can focus attention on security in general or some narrow aspect of security (e.g., the dangers of opening an unknown email or attachment, or how to maintain laptop security while traveling).

The failure to provide IT security training and raise awareness increases the risk that users will not understand their responsibilities, putting the data and IT resources with which they have been entrusted at greater risk for unauthorized access, misuse or abuse. For example, without training and awareness, employees may not understand how their Internet browsing could cause their computers to become infected with malicious software that may compromise any personal, private or sensitive information residing on them.

Local government and school officials sometimes say that they cannot afford the cost of IT security training and awareness. Fortunately, there are a number of no-cost or low-cost solutions available from a variety of sources. The following organizations offer free or low-cost IT security training and awareness materials:

Center for Internet Security	**https://www.cisecurity.org/**
New York State Education Department	**http://www.nysed.gov/data-privacy-security**
New York State Office of Information Technology Services	**https://its.ny.gov/**
New York State Office of the State Comptroller	**https://www.osc.state.ny.us/**
United States Cybersecurity and Infrastructure Security Agency	**https://www.cisa.gov/**

Municipal and school associations (e.g., New York Conference of Mayors, New York State School Boards Association) also periodically offer low-cost IT security training.

Lastly, developing and delivering IT security training and maintaining IT security awareness does not have to be a formal, elaborate and expensive endeavor. It can be as simple as gathering staff together to review your policies collectively and having a roundtable discussion on security matters applicable to your computing environment. The discussions could center on one or more of the following issues:

- Emerging trends in information theft and other social engineering reminders;
- Limiting the type of personal, private and sensitive information collected, accessed or displayed to that which is essential for the function being performed;
- The dangers of downloading files and programs from the Internet;
- How to respond if malware or an information security breach is detected;
- Other key IT security controls such as strong passwords, malware protection or wireless security.

Awareness efforts could also include disseminating the free security alerts from the organizations mentioned above or sending out periodic security reminders via email that address some aspect of your IT security policy.

Your personnel should understand their IT responsibilities, be knowledgeable about potential threats and be prepared to respond appropriately to everyday challenges, as well as less frequent events, such as the loss of personal information. The growing availability and ease of obtaining free- and low-cost training and awareness materials eliminates excuses for not having a well-informed workforce.

IT security training and awareness is an essential part of protecting computer systems and data. Your personnel should understand their IT responsibilities, be knowledgeable about potential threats and be prepared to respond appropriately to everyday challenges, as well as less frequent events, such as the loss of personal information. The growing availability and ease of obtaining free- and low-cost training and awareness materials eliminates excuses for not having a well-informed workforce.

Area #3 – Computer Hardware, Software, and Data Inventories

Local governments and schools should maintain detailed, up-to-date inventory records for all computer hardware, software and data. The information maintained for each piece of computer equipment should include a description of the item including the make, model and serial number; the name of the employee to whom the equipment is assigned, if applicable; the physical location of the asset; and relevant purchase or lease information including the acquisition date. Software inventory records should include a description of the item including the version and serial number, a description of the computer(s) on which the software is installed and any pertinent licensing information.

In addition to hardware and software inventories, organizations should maintain an inventory of information assets (i.e., data) that classifies the data according to its sensitivity and identifies where the data resides (e.g., servers, desktops, laptops, USB flash drives and cloud or other third-party storage locations). Because different kinds of information require different levels of protection, the nature of the data has to be evaluated so that appropriate internal controls can be established and monitored. Data classification is the process of assigning data to a category that will help determine the level of internal controls over that data. In some instances, laws, regulations or an organization's policies predefine the classification of each data type. Here is an example of a data classification scheme:

Because different kinds of information require different levels of protection, the nature of the data has to be evaluated so that appropriate internal controls can be established and monitored.

- **Public** – Information that is widely available to the public through publications, pamphlets, web content and other distribution methods.
- **Internal Use** – Routine operational information that is not approved for general circulation and where unauthorized access, modifications or disclosure would be inconvenient but not result in financial loss or damage to public credibility. Examples include routine correspondence, employee newsletters, internal phone directories and internal policies and procedures.
- **Confidential** – Confidential data is information that, in the event of unauthorized access, modifications or disclosure, could result in significant adverse impacts on a local government's or school's ability to perform critical work or compromise the integrity of the local government or school, its employees, its customers or third parties. Examples include data used to produce payroll or vendor payments, preliminary drafts of bid specifications and employee system passwords. It also includes any information concerning a person that can be used to identify or assume the identity of the individual. Examples include Social Security numbers and the combination of name, address and date of birth.
- **Restricted Confidential** – Information where loss, unauthorized modification or disclosure is likely to result in the most serious impacts to a local government's or school's ability to fulfill its responsibilities. Examples include the local government's or school's strategy for defending lawsuits, preliminary investigation results and assessments of security vulnerabilities.

Local governments and schools cannot properly protect their IT resources, including data, if they do not know what resources they have and where those resources reside. The failure to maintain detailed, up-to-date hardware, software and data inventory records exposes these valuable assets to an increased risk of loss, theft or misuse. For example, State Education Law and Regulations require[9] that no student data be shared with third parties without an agreement that complies with federal and State laws. Without awareness of the student data that exists, schools cannot guarantee compliance with the law's requirements.

Similarly, without proper identification of all devices on a network, unauthorized devices and software can be easily introduced, putting local government or school data at risk. A single compromised device can become a launching point for further network attacks, quickly turning one compromised computer into many. Furthermore, accurate inventory records are essential for effective patch management (see Area #6 – Patch Management) and software licensing compliance.[10] Incomplete or outdated records makes it unlikely that software patches necessary to address known security vulnerabilities can be applied on a timely basis, if at all. In addition, insufficient records increase the likelihood that you may inadvertently violate copyright laws by having more software users than licenses for a particular application and incur penalties as a result. The accuracy of inventory records should be verified through periodic physical inventories.

Local governments and schools cannot properly protect their IT resources, including data, if they do not know what resources they have and where those resources reside.

Area #4 – Contracts and Service Level Agreements for IT Services

Local governments and schools increasingly rely on third parties to provide a variety of IT-related services. For your protection and to avoid potential misunderstandings, there should be a written agreement between your local government or school and the IT service provider that specifies the level of service to be provided by the vendor and clearly states your needs and expectations including those relating to the confidentiality and protection of personal, private and sensitive information.

In addition, it is very important for local governments and schools to know who (any vendor or sub-contractor) has access to its personal, private and sensitive information, and to convey the security expectations to those vendor(s) and sub-contractor(s) through the written contract(s). Any legal requirements relating to the protection of specific type(s) of data (for example, PII or electronic health records) should also be considered, discussed with the vendor and included in the contract, as appropriate.

[I]t is very important for local governments and schools to know who (any vendor or sub-contractor) has access to its personal, private and sensitive information, and to convey the security expectations to those vendor(s) and sub-contractor(s) through the written contract(s).

State Education Law and Regulations require educational agencies to include the following in any contract that involves sharing student, teacher or principal (shared) PII with the third-party contractor:[11]

- A requirement to maintain the confidentiality of shared PII.
- A bill of rights supplement that specifies (among other things):
    - The exclusive purposes for which shared PII will be used.
    - The contract's duration and a description of what will happen to shared PII upon the contract's expiration (e.g., whether, when and in what format it will be returned and/or whether, when and how it will be destroyed).
    - How shared PII will be protected using encryption while in motion and at rest.
- The contractor's data security and privacy plan that includes (among other things):
    - The administrative, operational and technical safeguards and practices to protect shared PII.
    - How officers and employees with shared PII access receive, or will receive, training on the laws governing confidentiality of that information.
    - Any use of subcontractors and how those relationships and contracts will be managed to ensure shared PII is protected.
    - How data security and privacy incidents that implicate shared PII will be managed, including any plans to identify breaches and unauthorized disclosures and to promptly notify the educational agency.

While contract terms begin to establish expectations, a service level agreement (SLA) should be used to help further expectation clarity and measurement methods. An SLA is different from a traditional written contract in that it should establish comprehensive, measurable performance targets and remedies for not meeting those requirements, so that there is a mutual understanding of the nature and required level of services to be provided. SLAs are a critical component of any IT system outsourcing or support contract. For example, if you contract with an IT vendor to administer patch management with the goal of ensuring that patches and updates that are released throughout the year are installed on a timely basis, the SLA should indicate exactly what operating system(s) and application(s) are covered and what "timely" means (e.g., is the expectation that patches be applied as soon as available, on a weekly basis or on a quarterly basis?). An SLA with a cloud service provider could, for example, indicate that you will have availability to an application 99.95 percent of the time and allow the municipality to reduce its payment by a given percentage if that percent is not achieved.

In our experience, many of the SLAs that local governments and schools enter into are vague in terms of the services contracted for and the expected quality of those services. Such vaguely worded agreements can, among other things, contribute to confusion over who has responsibility for various aspects of the IT environment (i.e., the local government/school or contractor), which ultimately puts the local government's or school's data and computer resources at greater risk for unauthorized access, misuse or loss. Generally speaking, the more specific the SLA, the better. There should be no uncertainty about what the contractor will deliver, when it will be delivered and how much it's going to cost. A vague agreement can lead to additional or increasing costs you were not expecting.

In our experience, many of the SLAs that local governments and schools enter into are vague in terms of the services contracted for and the expected quality of those services.

Many IT service providers have standard SLAs – reflecting various levels of service at different prices – that can be a good starting point for negotiation. SLAs should be reviewed by the local government's or school's legal counsel and IT staff, as appropriate. They should also be periodically reexamined, especially if your IT environment or needs change significantly. Developing a good SLA takes some effort but can help avoid potentially costly misunderstandings and establish an efficient and secure computing environment.

Finally, local governments and schools should consult New York State Archives[12] guidance prior to entering into contracts, especially those relating to data storage services.

Area #5 – Malware Protection

Malicious software, or malware, are software programs that are designed to harm computer systems. These programs can wreak havoc on both systems and electronic data by, for example, gathering sensitive information such as passwords without the computer user's knowledge, deleting files and making systems inaccessible or inoperable. Computer users can inadvertently install malware on their computers by opening email attachments, downloading content from the Internet or merely visiting infected websites. Damage caused by malware can be expensive to fix and can cause significant losses in productivity until corrected. This is especially true with the ongoing and increasingly sophisticated threat of ransomware attacks against local governments and schools.

These programs can wreak havoc on both systems and electronic data by, for example, gathering sensitive information such as passwords without the computer user's knowledge, deleting files and making systems inaccessible or inoperable.

One way to detect and stop some forms of malware before it can affect its targets is by using antivirus software. Antivirus software should be installed and kept current with software and signature (a set of characteristics also referred to as virus definitions)

updates. Antivirus software should be set to update definitions daily and to scan for threats throughout the day. Without current virus definitions, protection is limited and leaves computers at risk of being compromised by new types of threats. Similarly, without ongoing scanning, threats could infect computers between scans and then disable antivirus software to avoid detection.

Some local governments and schools use a mix of purchased and free antivirus software (downloaded from the Internet). While there is nothing inherently wrong with using different kinds of antivirus software, it may make timely, coordinated management of antivirus protection more challenging. If a local government or school chooses to use free antivirus software, officials should carefully consider all terms defined by licensing agreements, including type and extent of the software's use, to ensure compliance.

In addition, some malicious programs are written to automatically propagate, or spread across, any new system they discover. Because malware can be embedded onto a wide variety of devices, a best practice is to force scans of any new devices connected to computers, such as USB flash drives and digital cameras, and turn off the AutoPlay[13] feature for such devices.

Area #6 – Patch Management

Patches update software programs and could help protect systems running those programs from attacks. A patch can be an upgrade (adding features), computer bug fix, new hardware driver installation or an update to address new issues, such as security or stability problems.

If patches are not installed regularly, the network and computers have an increased risk of vulnerability to viruses and other problems because known problems with software are not corrected. Because attackers are aware of these potential weaknesses, they can look for and exploit unpatched software.

Additionally, when vendors stop supporting certain software versions, they may stop providing technical support or bug and security fixes (patches) for those versions. Without ongoing updates, security weaknesses and bugs in the software can be exploited by attackers in a wide range of ways.

Many unsupported and outdated software programs have vulnerabilities that were previously discovered and are well known by attackers. Code to exploit some of those vulnerabilities is freely available on the Internet and could allow attackers to gain unauthorized access and inappropriately modify or steal data residing on vulnerable computers.

Area #7 – Access Controls

IT access controls prescribe who or what computer process may have access to a specific IT resource, such as a particular software program or database. For example, access controls can be implemented to limit who can view electronic files containing employee names and Social Security numbers. The first step in implementing adequate access controls is determining what level and type of protection is appropriate for various resources (e.g., data) and who needs access to these resources. The objectives of limiting access are to ensure:

- Outsiders (e.g., attackers) cannot gain unauthorized access to your systems or data,
- Access to sensitive resources (e.g., operating systems, security software programs) is limited to very few individuals who have a valid business need for such access, and
- Employees and contractors are restricted from performing incompatible functions or functions beyond their responsibilities.

The first step in implementing adequate access controls is determining what level and type of protection is appropriate for various resources (e.g., data) and who needs access to these resources.

There should be written procedures in place for granting, changing and revoking access to the network, individual computer systems and specific software applications. These procedures should establish who has the authority to grant or change access (e.g., department manager approval) and allow users to access only what is necessary to complete their job duties and responsibilities. Furthermore, you should establish and follow a process for revoking access by immediately disabling unneeded user accounts and removing unneeded user permissions. For example, former employees' accounts should be disabled on the day they leave local government or school employment and transferred employees' permissions should be adjusted on the day the transfer is effective.

You should periodically compare the list of current active employees (i.e., employee master list) to the list of network user accounts to determine if user accounts belong to current employees. Any user account not belonging to a current employee should be evaluated and any account that cannot be associated with an authorized user or process should be disabled. After an account is disabled, any files associated with that account should be moved to a secure file server for analysis by IT or management personnel. Where possible, system administrators should monitor attempts to access disabled accounts through audit logging.

Access should be assigned within the network based upon what resources users need to complete their job duties and responsibilities. For example, if there are shared folders on the network, users within the highway department should only have access to the folders they need, which would most likely not include the personnel department's folders. Likewise, individuals with accounting duties should only have access to the portion of your financial accounting system they need to perform their job.

Access should be assigned within the network based upon what resources users need to complete their job duties and responsibilities.

To help ensure individual accountability within the network, every user should have and use their own network user accounts (usernames and passwords). Likewise, to help ensure individual accountability within software applications, every user should have and use their own application user accounts (usernames and passwords). If users share accounts, accountability could be diminished and activity in the system may not be able to be traced back to a single user.

Also, users should be able to set their own passwords. If passwords are set for users, there is limited accountability because someone else knows the password.

Holding passwords to certain requirements makes them more difficult to crack or guess. Here are some criteria you should consider with regard to passwords:[14]

- **Length** – Passwords should be at least eight characters in length. Password length has been found to be a primary factor in characterizing password strength. As the number of characters in a password increases, the strength of the password increases exponentially. For example, an eight-character password has 78 million times the possible combinations than that of a four character password; in terms of time, that is 1 second versus 903 days.

- **Complexity Requirements** – A complex password should contain at least one uppercase character, one lowercase character, one numeric character and one special character (e.g., %, #, @) and not include names or words that can be easily guessed or identified using a password-cracking mechanism or dictionary. Furthermore, the password should not contain any part of the name of the account, network, local government or school.

- **Aging** – Passwords should be changed every 60 days or less. Less frequently changed passwords are at greater risk of being guessed and used by attackers for unauthorized access.

- **Failed Log-On Attempts** – To prevent password guessing and online password attacks, failed log-on attempts should be limited to 10 or fewer consecutive failed attempts, after which the system should automatically lock users out for a duration of at least 15 minutes or until an administrator manually unlocks them before they are able to attempt another log-on.

Schools should be aware that State Education Law and Regulations[15] require student PII be password protected when transmitted electronically to parents or eligible students.

Area #8 – Online Banking

Fraud involving the exploitation of valid online banking credentials is a significant risk facing any local government or school that processes financial transactions online. Some of the more popular types of electronic fraud targeting online banking are phishing[16] and malware.[17] In a typical scenario, the targeted individual (or group of individuals) receives an email that either contains a malicious attachment or directs the recipient to a malicious website. Once the recipient opens the attachment or visits the website, malware containing a key logger or other data harvesting and reporting mechanism is installed on the recipient's computer, or the recipient is prompted to input their username and password, which are collected for malicious use. A key logger collects login information, allowing the perpetrator to impersonate the legitimate user or create another user account with access to the victim's online bank accounts. Thereafter, fraudulent electronic transfers are initiated and directed to bank accounts in the United States or foreign countries.

Despite financial institutions' security controls, there is no way to guarantee the safety of online banking. The tactics used to commit fraud can range dramatically in sophistication and continually evolve over time. Likewise, there is no single control that is most effective against cyberattacks. A best practice for protecting IT systems, information and local government and school resources is to build successive layers of defense mechanisms, a strategy referred to as defense-in-depth, a concept discussed earlier in this document.

> Local governments and schools should have a combination of nontechnical and technology-based controls in place to safeguard against online banking fraud.

Local governments and schools should have a combination of nontechnical and technology-based controls in place to safeguard against online banking fraud. For example, officials should establish written policies and provide recurring information security awareness training to all employees who use computers connected to the Internet or the local government or school's network. In addition, malware protection should be kept up-to-date and, whenever possible, a wired rather than wireless network should be used for financial transactions. If a wireless network must be used, certain security measures should be in place (see Area #9 – Wireless Network)

> The ease and speed with which large amounts of money can be transferred among accounts and banks requires heightened attention to traditional internal controls, such as the proper segregation of incompatible duties and timely reviews of online banking transactions.

Although online banking fraud is often committed by external parties, risks posed by employees must also be considered. The ease and speed with which large amounts of money can be transferred among accounts and banks requires heightened attention to traditional internal controls, such as the proper segregation of incompatible duties and timely reviews of online banking transactions. It is also critical that bank accounts be frequently monitored for unauthorized or suspicious activity. Any suspicious activity should be immediately reported to banking officials and/or law enforcement. The window of time in which recoveries can be made from fraudulent online banking transactions is limited, and a rapid response may prevent additional losses.

A further discussion of online banking controls can be found in the Office of the State Comptroller's publication entitled *Local Government Management Guide: Cash Management Technology*.[18]

Area #9 – Wireless Network

Wireless networks are exposed to many of the same types of threats and vulnerabilities as wired networks, including viruses, malware, unauthorized access and data loss. However, they are considered inherently less secure than wired networks because data are transmitted into the air and can potentially be intercepted and misused by individuals with malicious intent. Also, because wireless networks are often used as extensions of wired networks, even minor IT security weaknesses on wireless networks can expose internal network resources to additional threats. Therefore, a wireless environment requires certain additional security precautions to prevent unauthorized access and eavesdropping.

Although wireless environments and their related security systems can be quite complex, local government and school personnel can implement effective controls with relative ease and without incurring additional costs. Some best practices relating to wireless technology include:

- Adopting written policies and procedures;
- Determining the optimal number, physical location and broadcasting power of wireless access points;
- Maintaining an inventory of and monitoring wireless access points;
- Changing the service set identifier (the SSID or name of the wireless network) using a naming convention that excludes identifiable information about the local government or school, location, technology, manufacturer and type of data traversing the network;
- Requiring an access password for users and enabling the most secure encryption available (currently WPA2 or WPA3);
- Changing the administrative password (used by the administrator to set up the wireless access point) from its well-known default value;
- Updating and patching all software and hardware devices in a timely manner; and
- Considering other security controls that may be necessary given the local government's or school's unique computing environment and security needs.

A further discussion of wireless technology and security can be found in the Office of the State Comptroller's publication entitled *Local Government Management Guide: Wireless Technology and Security*.[19]

Area #10 – Firewalls and Intrusion Detection

Networks that are connected to the Internet are physically connected to unknown networks and their users all over the world. While such connections are often useful, they also increase the vulnerability of IT systems and electronic data to access and attacks from unauthorized individuals.

Firewalls

Firewalls are hardware and/or software programs that enforce boundaries between devices on different networks or network segments. Firewalls control network communications, using rules that specify which communication types are allowed between and within boundaries and which are denied. To safeguard against unauthorized access and disruption, the network administrator should configure firewall rules to allow only those communications types that are needed for system operations and explicitly deny all other communications.

Firewalls can also act as effective tracking tools because they can perform important logging and auditing functions. For these reasons, the network administrator should enable firewall logs and periodically review logged activities/events.

There are several types of firewalls, each with varying capabilities to analyze network communications and allow or deny specific types by comparing communication characteristics to defined rules. Understanding the capabilities of each type of firewall, acquiring firewall technologies and designing firewall rules that effectively address a local government's or school's needs are critical to achieving protection for network communications.

Firewalls are hardware and/or software programs that enforce boundaries between devices on different networks or network segments.

There are many aspects to firewall management. For example, choosing the type(s) of firewall to use and where to position each within the network can significantly affect the rules that the firewalls can enforce. Firewall rules may need to be updated as the local government's or school's requirements change, such as when new applications or devices are added to the network.

Firewall performance also needs to be monitored so that potential resource issues can be identified and addressed before components become overwhelmed. Logs and alerts that firewalls generate should also be continuously monitored to identify attempts to bypass network security controls—both successful and unsuccessful. Given their potential impact to security and operations, firewall rules should be managed using a formal change-management control process, with rule reviews or tests performed periodically to ensure continued compliance with the local government's or school's policies. Like any software, firewall software should be patched regularly as vendors provide updates to address vulnerabilities and improve functionality.

Intrusion Detection

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of a violation of computer security policies, acceptable use policies or standard security practices. Certain aspects of intrusion detection can be automated with modern antivirus software, firewalls or dedicated intrusion detection systems (IDSs). Network-based IDSs capture and analyze network communications within a network or network segment, while host-based IDSs capture and analyze activity to and from a particular computer.

Because the log information maintained may be too voluminous to review on a routine basis, the IDS should be implemented to selectively identify unauthorized, unusual and sensitive access activity, such as:

- Attempted unauthorized access,
- Deviations from access trends (e.g., access during off-hours),
- Access to sensitive data and resources,
- Highly sensitive privileged access, such as the ability to override security controls,
- Floods of data coming from or going to a particular system or group of systems,
- Access modifications made by security personnel, and
- Multiple consecutive unsuccessful attempts to log-on to a system.

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of a violation of computer security policies, acceptable use policies or standard security practices.

Unauthorized, unusual or sensitive access activity identified by the IDS should be reviewed and any apparent or suspected violations should be investigated. It is important to note that seemingly innocuous or legitimate behavior could be a manual probe to collect data about a network or security over a network, possibly for the purposes of formulating an attack plan for that network. Therefore, it is important that you provide for a periodic manual review of network activity even with an automated IDS in place.

When a security violation occurs, appropriate action should be taken to identify and remedy the internal control weaknesses that allowed the violation to occur, repair any damage that has been done, determine whether the violation constitutes a breach requiring notification of affected individuals and, when feasible, identify and discipline the perpetrator.

It is important that a local government or school have formal written procedures for reporting security violations or suspected violations to the IT manager or other appropriate personnel so that multiple related incidents can be identified, other employees can be alerted to potential threats, and appropriate investigations can be performed. Such incidents might include multiple attacks by a common hacker or repeated infections with the same malicious software.

Area #11 – Physical Controls

Physical security controls restrict physical access to computer resources and protect these resources from intentional or unintentional harm, loss or impairment. Such controls include guards, gates and locks, and also environmental controls such as smoke detectors, fire alarms and extinguishers, protection from water damage and uninterruptible power supplies.

Larger local governments and schools may have a server room while smaller units may place servers next to or under a desk, in a closet, in the middle of the room or other high-traffic area. You should inspect the location of computers and server areas/rooms and ensure that there are adequate physical security controls commensurate with the risks of physical damage or access.

Physical security controls restrict physical access to computer resources and protect these resources from intentional or unintentional harm, loss or impairment.

Area #12 – Information Technology Contingency Planning

Written IT Contingency Plan

Because no computer system can be expected to operate perfectly at all times, unplanned service disruptions are inevitable. A disruptive event could include a natural disaster such as a flood or fire, or something more localized such as a computer virus or ransomware infection. The plans, policies, procedures and technical measures that help enable the recovery of operations after an unexpected IT disruption are collectively referred to as IT contingency planning.

An unplanned IT disruption involving the corruption or loss of data or other computer resources from ransomware, hardware failure or human error, for example, could significantly curtail a local government's or school's operations. Proactively anticipating and planning for such disruptions will prepare local government and school personnel for the actions they must take in the event of a disruption and could significantly reduce the resulting impact.

Proactively anticipating and planning for such disruptions will prepare local government and school personnel for the actions they must take in the event of a disruption and could significantly reduce the resulting impact.

The goal of IT contingency planning is to help enable an IT system and/or electronic data to be recovered as quickly and effectively as possible following an unplanned disruption. The content, length and resources necessary to prepare an IT contingency plan will vary depending on the size and sophistication of your local government's or school's operations.

Some best practices relating to IT contingency planning include:

- Assembling a team responsible for drafting the plan,
- Identifying and prioritizing critical business processes and services,
- Developing and distributing the plan to all responsible parties,
- Training personnel expected to execute the plan,
- Testing the plan as appropriate, and
- Reviewing and revising the plan as necessary to ensure it still meets local government or school needs.

Backup Procedures

A backup is a copy of data files and software programs made to replace original versions if there is loss or damage to the original. Establishing backup procedures is a necessary part of IT contingency planning and often critical for restoring operations quickly and effectively following an IT disruption.

Some best practices relating to backup procedures include:

- Adopting a backup policy that defines the responsibility, frequency, scope, storage location(s) and specific method(s) for backups;
- Backing up data at intervals appropriate for the local government's or school's data needs and usage;
- Verifying data has been backed up and can be restored whenever needed; and
- Storing backups in an offline and offsite location that meets the local government's or school's data security requirements.

Establishing backup procedures is a necessary part of IT contingency planning and often critical for restoring operations quickly and effectively following an IT disruption.

A further discussion of IT contingency planning and backup procedures can be found in the Office of the State Comptroller's publication entitled *Local Government Management Guide: Information Technology Contingency Planning*.[20]

Additional Resources

Center for Internet Security	https://www.cisecurity.org/
National Institute of Standards and Technology	https://www.nist.gov/
New York State Education Department	http://www.nysed.gov/data-privacy-security
New York State Office of Information Technology Services	https://its.ny.gov/
New York State Office of the State Comptroller	https://www.osc.state.ny.us/
United States Cybersecurity and Infrastructure Security Agency	https://www.cisa.gov/

Information Technology Governance

Security Self-Assessment

Date completed: _____

***Note: This document may be confidential/restricted confidential upon completion. Please handle accordingly.**

		YES	NO	N/A
IT Policy				
1a	Are IT policies adopted, distributed and updated as necessary?			
	List policies, their (physical or electronic) locations and the dates adopted and last revised:			
1b	Was a breach notification policy adopted?			
	Date adopted: Date last revised:			
1c	Was a data security and privacy policy adopted?			
	Date adopted: Date last revised:			

IT Security Training and Awareness				
2a	Were all computer users provided IT security training?			
	Date(s) of training:			
	Who attended the training:			
2b	Have all officers and employees with access to personally identifiable information (PII), and in addition 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?			
	Date(s) of training:			
	Who attended the training:			
2c	Are there other efforts to raise IT security awareness?			
	Describe awareness efforts:			
Computer Hardware, Software and Data Inventories				
3a	Is a detailed, up-to-date inventory of computer hardware maintained?			
	Review a copy of the hardware inventory and note when last updated:			

3b	Is a detailed, up-to-date inventory of authorized software maintained?			
	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?			
	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?			
	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?			
	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?			
	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?			
	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?			
5c	Is the AutoPlay feature turned off (e.g., in network security settings) for all removable devices?			
Patch Management				
6	Are operating system and other software programs maintained at vendor-supported versions and are patches and updates applied and installed in a timely manner?			
	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?			
7b	Are unique application user accounts created for each user where applicable?			
7c	Do any accounts exist that cannot be tied to an authorized user or process?			
	Describe the process for disabling unneeded user accounts:			
7d	Is a current list of authorized users and their levels of access maintained and periodically removed?			
	Review the list of authorized users and their levels of access.			
7e	Are passwords held to length and complexity requirements?			
	Describe the requirements:			
7f	Are password changes enforced every 60 days or less?			
	Indicate how often passwords are changed and describe how the change is enforced:			
Online Banking				
8a	Do you have an online banking policy?			
	Review the policy.			

8b	Are online banking duties properly segregated?			
	Who has access to prepare, approve, process and record transactions for each online bank account?			
8c	Are online bank accounts monitored?			
	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?			
	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?			
	What is/are the SSID(s)?			
9c	Is the most secure encryption available used?			
	Note type of encryption used:			

Firewalls and Intrusion Detection				
10a	Is a firewall(s) in place to control network communications?			
	Who is responsible for maintaining firewall rules and settings?			
10b	Are firewall activities/events logged?			
	Who reviews the logs?			
10c	Has intrusion detection been automated using modern antivirus software, a firewall(s) or a dedicated intrusion detection system (IDS)?			
	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?			
	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?			
11c	Is there an uninterrupted power source?			

11d	Are inspections conducted for physical security control weaknesses?			
	Who conducted the last inspection and on what date?			
Information Technology Contingency Planning				
12a	Has an IT contingency plan been developed?			
	Review the plan and note the date adopted:			
12b	Has the plan been distributed to responsible parties?			
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?			
	Date plan last revised:			
12e	Are all critical data files and software programs periodically backed up?			
	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?			
	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?			

Notes

[1] A type of malicious software that prevents access to a computer or electronic device demanding that a ransom payment be made.

[2] Pursuant to Section 208, notification is required to be given to certain individuals when there is a "breach of the security of the system" as it relates to "private information." "Breach of the security of the system" is generally defined as meaning unauthorized acquisition of computer data which compromises the security, confidentiality or integrity of personal information maintained by the entity. "Private information" is defined as personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired: (1) Social Security number; (2) driver's license number or non-driver identification card number; or (3) account number, credit or debt card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

[3] Education Law Section 2-d(5)(c); 8 NYCRR 121.5(b)

[4] 8 NYCRR 121.5(c)(1)

[5] 8 NYCRR 121.5(c)(2)

[6] Mobile devices include, but are not limited to, laptops, tablets, smartphones, USB (universal serial bus) flash drives and memory cards.

[7] 8 NYCRR 121.7

[8] Social engineering refers to the methods attackers use to deceive victims into performing an action such as opening a malicious webpage or running an unwanted file attachment. Many social engineering efforts are focused on tricking users into disclosing usernames and passwords.

[9] Education Law Sections 2-d(5)(e), (f); 8 NYCRR 121.2(c)

[10] Software typically comes with a license that grants end-users permission to use one or more copies of the product. Local governments and schools should closely track their license usage to help ensure they do not inadvertently utilize software in a manner that might constitute copyright infringement. The illegal use or distribution of software, known as software piracy, can result in considerable penalties.

[11] Education Law Section 2-d(3)(c); 8 NYCRR 121.2(c), 121.3(c), 121.6(a)

[12] **http://www.archives.nysed.gov/**

[13] A feature built into Windows operating systems to automatically "play" files stored on devices when connected to computers. This feature poses a security risk because malicious programs could be embedded on connected devices.

[14] While the National Institute of Standards and Technology updated its password guidance (Special Publication 800-63B: Digital Identity Guidelines) and no longer recommends requiring complex or arbitrarily changed passwords, it now recommends additional compensating controls including a requirement to compare and reject passwords known to be commonly used, expected or compromised. Unless these compensating controls are implemented, passwords should be complex and changed every 60 days or less.

[15] Education Law Section 2-d(3)(b)(3); 8 NYCRR 121.12(f)

[16] Phishing attacks use fake email messages or other techniques, sometimes pretending to represent a bank, to trick you into providing personal or financial information. The email may provide links to a counterfeit website and request information such as name, password, and account number.

[17] Malware is malicious software (e.g., ransomware, viruses, Trojans, spyware, rootkits, and worms) that typically is installed without the user's knowledge or consent. Such software is specifically designed to harm computer systems and electronic data, often by deleting files, gathering sensitive information, or making systems inaccessible or inoperable. The different types of malware can capture keystrokes for login information, monitor and capture other data to authenticate identity, generate web pages that appear to be legitimate but are not and hijack a browser to transfer funds without the user's knowledge.

[18] **https://www.osc.state.ny.us/files/local-government/publications/pdf/cashtechnology.pdf**

[19] **https://www.osc.state.ny.us/localgov/pubs/lgmg/wirelesstechnologysecurity.pdf**

[20] **https://www.osc.state.ny.us/localgov/pubs/lgmg/itcontingencyplanning.pdf**

Contacts

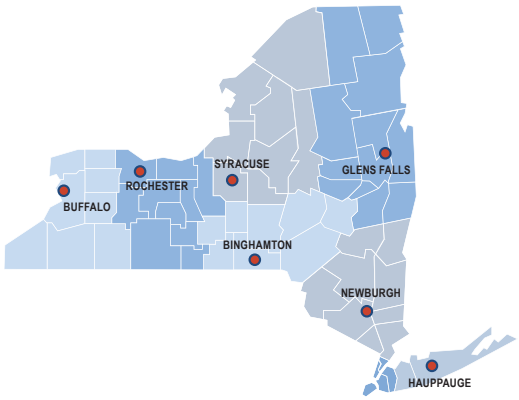
Office of the NEW YORK STATE
COMPTROLLER

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.state.ny.us/local-government



Andrea C. Miller
Executive Deputy Comptroller

Executive • 518.474.4037
Elliott Auerbach, Deputy Comptroller
Tracey Hitchen Boyd, Assistant 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, 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, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington

HAUPPAUGE REGIONAL OFFICE
Tel 631.952.6534 • **Fax** 631.952.6091 • **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: Columbia, Dutchess, Greene, 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, Chemung, 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 315.793.2484

Contact

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

110 State Street, 12th floor
Albany, NY 12236
Tel: (518) 474-4037
Fax: (518) 486-6479
or email us: localgov@osc.ny.gov

www.osc.state.ny.us/local-government

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller

Released March 2012
Updated December 2021