Information Technology Governance

Security Self-Assessment

Date completed: _____

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 be downloaded at
https://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

		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 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 reviewed?			
	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?			
	Describe expectations and how those expectations are communicated:			
7f	Have password requirements been defined related to for example, password comparisons, invalid attempts or encryption?			
	Identify the requirements and describe how each 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?			

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 be downloaded at

https://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