Ins and Outs of a Tech AUDIT

2018

Presentres:

Florida's Technology Department

Rudy Gordon- Computer Network Specialist (Here in spirit)

Dana Castine- Director of Math, Science, Technology

Florida Union Free School District Information

- 2 School Buildings
- Approx. 825 Students Pre-K-12
- Approx. 175 Staff Members
- 6 Administrators
- Approx. 40% Free and Reduced Lunch
- 1:1 Chromebook District
- Deployed 825 Chromebooks- 420 6-12 graders take device home
- Located in Orange County, Town of Warwick, Village of Florida
- Approx. 60 minutes NW of NYC
- Known as Onion Capital of the World
- Home of Jimmy Sturr, Polka King and William Henry Seward, US Secretary of State under President Lincoln- Purchased Alaska
- Home of the mighty Spartans, #WeAreFloridaNY, @FUFSD

What Would You Do?

Florida's Audit Key Findings and Recommendations

Audit Period- July 1, 2015-June 9, 2017

Key Findings

- Employees do not comply with the District's acceptable use policy.
- Controls over the collection, processing, transmission and storage of personal, private and sensitive information (PPSI) have not been developed.
- The District does not have service level agreements for services provided by OUBOCES and MHRIC, which could lead to confusion over roles and responsibilities of each party.

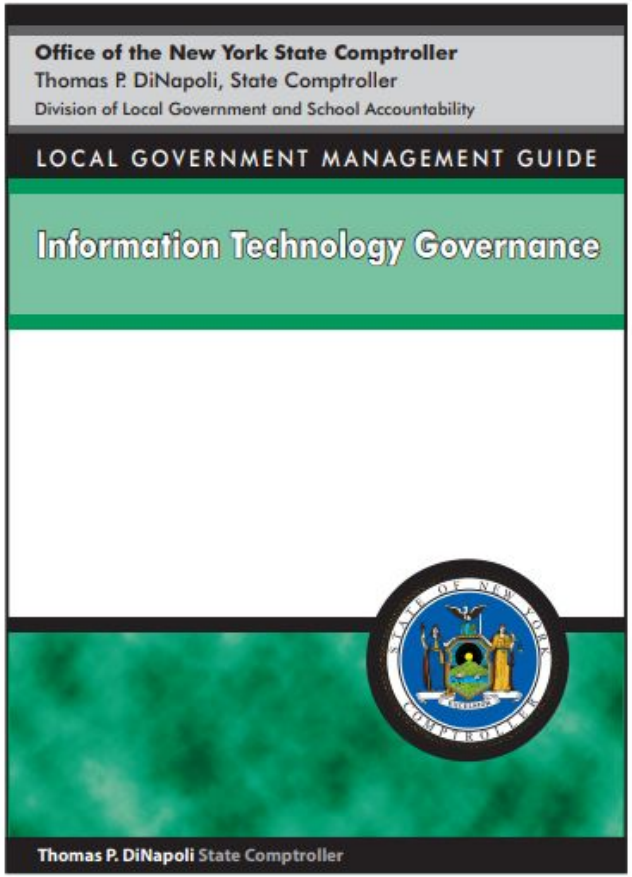
Key Recommendations

- Review and monitor employees' computer use to ensure compliance with the District's acceptable use policy.
- Inventory, classify and develop controls over PPSI maintained and collected by the District.
- Ensure that all IT services are provided based on a formal service level agreement.

IT Security: Top 12 Areas of Concern

Link to IT Governance Document:

https://www.osc.state.ny.us/localgov/pubs/lgmg/itgovernance.pdf



Contents of It Governance Document

12 Areas of Concern

Security Self-Assessment

Table of Contents

Internal controls

Policies

Procedures

Activities to designed to provide reasonable assurance that operations are going according to plan.

Secure All Data

Secure Financial Systems

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.

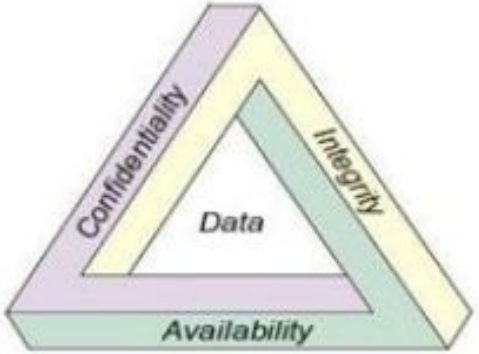
IT Security Fundamentals

CIA Triad- industry standard

Internal Controls:

- Data Security
- Network Security
- System 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 power outages, natural disasters, hardware failures, systems upgrades, and attempts by individuals with malicious intent to cause disruption.

Guidance for IT Security: Top 12 Areas of Concern

Area #1- IT Policy

To include but not limited to:

- Breach Notification Policy
- Internet, Email, and Personal Computer Use
- Use of and Access to Personal, Private and Sensitive Information
- Password Security
- Wireless Security Policy
- Mobile Computing and Storage Device Policy
- Online Banking

Guidance for IT Security: Top 12 Areas of Concern

Area #1- IT Policy- ACTIONABLES

- Policy Review!
- Remind staff there is no expectation of privacy
- Follow most up-to-date password complexity
- Procedures for mobile devices, online banking, etc…
- Means to identify, inventory and classify PPSI

Look at policies- NYS Office of Information Technology Services- https://its.ny.gov/tables/technologypolicyindex

Guidance for IT Security: Top 12 Areas of Concern

Area #2- Security Training and Awareness

- Protect the confidentiality, integrity and availability of data
- Training should:
  - Explain proper use of rules and behavior
  - Communicate policies and procedures
  - Be job specific ie:District Treasurer

Guidance for IT Security: Top 12 Areas of Concern

Area #2- Security Training and Awareness- Actionables

- Recommended Sites:
  - Center for Internet Security: https://www.cisecurity.org/
  - Industrial control Systems Cyber Emergency Response Team: https://ics-cert.us-cert.gov/
  - NYS Office of Information Technology Services: https://its.ny.gov/
  - NYS Office of the State Comptroller: https://www.osc.state.ny.us/
  - TEEX Domestic Preparedness Campus: https://teex.org/pages/homeland-security.aspx
  - US Computer Emergency Readiness Team: https://www.us-cert.gov
- Take staff attendance for ALL in-person Training
- KnowBe4: https://www.knowbe4.com/
- RIC One: http://www.ricone.org/

Guidance for IT Security: Top 12 Areas of Concern

Area #3- Computer Hardware, Software, and Data Inventories- Actionables

- Up-to-Date inventory for all Computer Hardware, Software, and Data
- Inventory information assets
  - Classify data
    - Public
    - Internal Use
    - Confidential
    - Restricted Confidential
- Complete Periodically
- Develop Processes and Procedures

Guidance for IT Security: Top 12 Areas of Concern

Area #4- Contracts for IT Services- Actionables

Components of an SLA should include:

Develop an SLA CheckList

- identification of the parties to the contract;
- definitions of terminology;
- term/duration of agreement;
- scope/subject;
- limitations (what, if anything, is excluded);
- service level objectives and performance indicators;
- roles and responsibilities;
- nonperformance impact;
- pricing, billing and terms of payment;
- security procedures; (PPSI)
- audit procedures;
- reporting;
- review/update and approvals. 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 costs or cost increases you were not expecting.

Guidance for IT Security: Top 12 Areas of Concern

Area #5- Virus Protection- Actionables

- User Training
- Update Antivirus Software
- Force scans of new external devices connected to computers

Guidance for IT Security: Top 12 Areas of Concern

Area #6- Patch Management- Actionables

Develop patch management policies and procedures

Patch, Patch, Patch, Patch, Patch...

Guidance for IT Security: Top 12 Areas of Concern

Area #7- Access controls- Actionables

- Do not provide access to systems beyond the job duty functions
- Develop a written process and procedure for assigning account access
- Refrain from assigning universal account access
- Automate Account access wherever possible
- Classlink’s Solutions- OneSync and OneRoster

Guidance for IT Security: Top 12 Areas of Concern

Area #8- Online Banking- Actionables

- Use the Defense-in-Depth Strategy- builds successive layers of defense mechanisms
- Use tech-based controls (up-to-date antivirus)
- Use non tech-based controls (written policies, training)
- Always use a hardwired computer for online banking
- Designate a computer used solely for online banking

Guidance for IT Security: Top 12 Areas of Concern

Area #9- Wireless Network- Actionables

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 organization, the location, technology, manufacturer and type of data traversing the network;
- Requiring an access password for users and enabling the most sure encryption available
- Changing the default administrative password used by the administrator who set up the wireless access point;
- Updating and patching all software and hardware devices;
- Considering other security controls that may be necessary given the organization's unique computing environment and security needs.

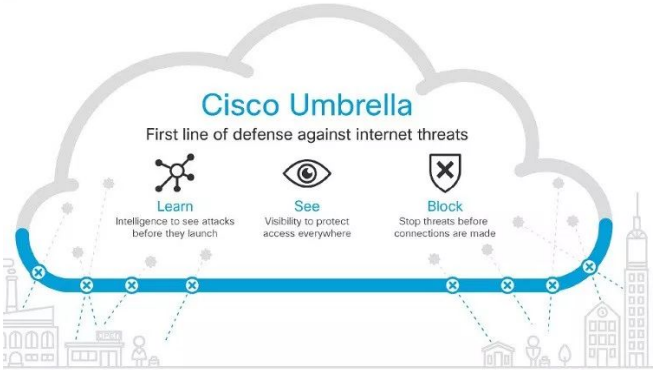
Guidance for IT Security: Top 12 Areas of Concern

Area #10- Firewall and Intrusion Detection- Actionables

Stop all unauthorized access!

Cisco- Firepower (IPS)

Cisco- Umbrella (DNS)



Guidance for IT Security: Top 12 Areas of Concern

Area #11- Physical Controls- Actionables

Protect MDF/IDF from excessive heat, water damage

Have an uninterruptible power supply

Provide limited physical access to MDF/IDFs

3rd Party Vendors

Guidance for IT Security: Top 12 Areas of Concern

Area #12- Written Contingency Plan- Actionables

Tests written plans, policies, procedures and technical measures to recover IT operations after an unexpected incident. Best practices include:

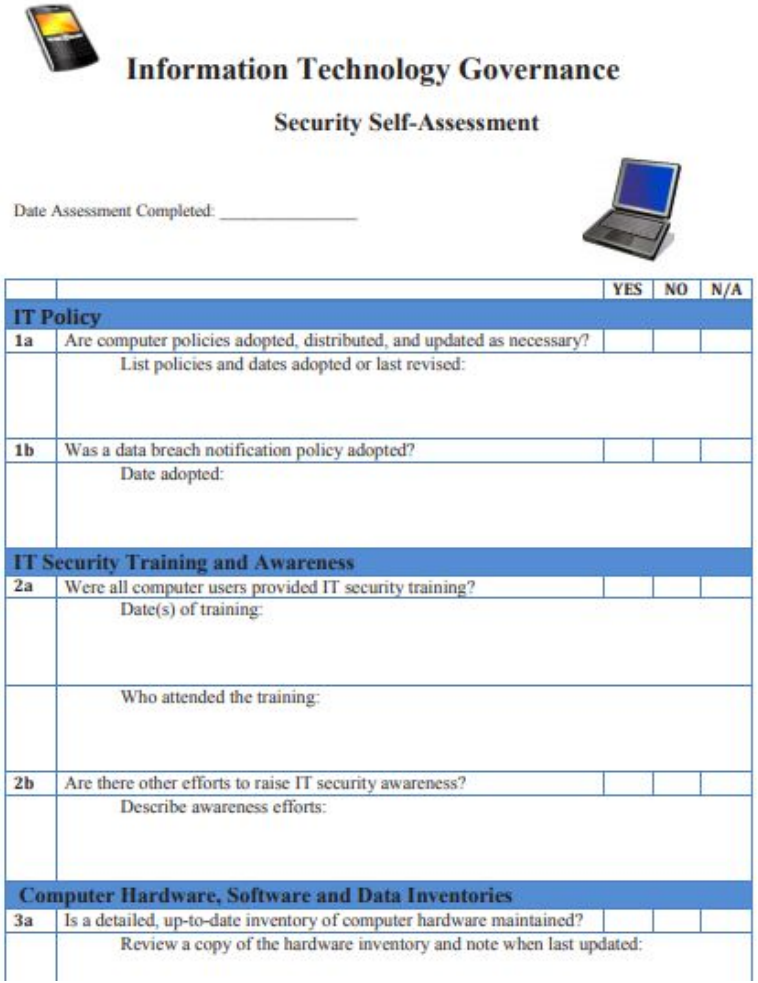
- adopting a data backup policy that defines the frequency and scope of backups, the location of stored backup data, the specific method for backing up;
- backing up data at regular intervals;
- verifying data has been backed up and can be restored in the event of an emergency;
- storing backups in an offsite location that meets the organization’s data security requirements

Security Self-Assessment

Addresses Key areas of Internal Controls such as:

- Policy
- Training
- Access
- Monitoring
- Review completed 1x/year

https://www.osc.state.ny.us/localgov/pubs/lgmg/itgovernance.pdf



Information Technology Governance

Security Self-Assessment

Date Assessment Completed: _____

		YES	NO	N/A
IT Policy				
1a	Are computer policies adopted, distributed, and updated as necessary?			
	List policies and dates adopted or last revised:			
1b	Was a data breach notification policy adopted?			
	Date adopted:			
IT Security Training and Awareness				
2a	Were all computer users provided IT security training?			
	Date(s) of training:			
	Who attended the training:			
2b	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:			

Questions???

Rudy Gordon-

rgordon@floridaufsd.org (845)651-3095 x30010

Dana Castine-

dcastine@floridaufsd.org (845)651-3095 x30006

Twitter:@danacastine