Section 23 – Information Technology

Overview

Information technology (IT) is most commonly used to refer to a system of computers and computer networks. IT is prevalent in local government operations of all sizes. Many government employees spend the vast majority of their workday on their computers. There are specialized software programs for just about any governmental activity or task, and large enterprise resource planning systems (ERP) that can coordinate all a government's data management needs. Employees draft correspondence on word processing software, do calculations and track management information on computer spreadsheets, and report to governing bodies with presentation software.

Employees use email, telephones, and the internet for communications, including telephony. They interface with the public through the local government's website, with other departments through fiber optic networks, and use internal and third-party secured portals for transferring money and other information.

Often these computer-assisted activities appear seamless to the users, but the computer hardware, software, networks, and processes must be installed correctly and managed properly to minimize disruptions and data loss, and to protect against unauthorized intrusion, data modification, and any other cybersecurity threats. Managing and maintaining the local government's information infrastructure is usually the responsibility of the organization's IT Department (ITD), but in small governments with no such department, it is often the responsibility of Finance.

The IT activities need support from the highest levels of the organization. Without proper funding for the maintenance of hardware, software, and the computer network, the organization risks: (1) becoming outdated, (2) data loss due to hardware failure, and (3) suffering from lack of interoperability between departments and other agencies.

Responsibilities of the Department

The ITD should provide a collaborative relationship with all departments by facilitating the identification of appropriate technology and assisting in the training and implementation of that technology. Written policies and procedures should be developed in all key IT areas. Goals and responsibilities of employees who oversee IT activities in the organization, may relate to the following areas:

- IT Management
- IT Hardware and Software Procurement
- Network Administration
- Application Installation/Development, Support, and Change Management
- Business Development
- Security

Following is a description of the duties with best practices in each of these areas.

1. **IT Management** – The IT Director or Manager oversees IT initiatives to ensure that all technology-related projects run smoothly and align with overall organizational policy. He/she performs strategic planning and recommends action for technology-related improvements.

Best Practices:

- Nurture a relationship with the organization's chief executive.
- Stay abreast of new developments in this ever-changing industry through conferences, publications, and blogs.
- Do not reinvent the wheel – see what others are doing.
- Establish and receive feedback from a user steering group.
- Work with departments to identify and prioritize critical business processes and services.

2. **IT Hardware and Software Procurement** – These ITD employees manage the acquisition and replacement of technology-related hardware, software, or services. They troubleshoot equipment errors and failures and handle the disposition of the equipment at the end of its useful life.

Best Practices:

- Acquire technology that aligns with organizational needs.
- Standardize hardware and software (including upgrades and options) to minimize incompatibility and maximize cross-agency usage.
- Centralize purchasing in IT to avoid duplication and encourage technical considerations.
- Maintain detailed, up-to-date inventory records for all computer hardware with identification numbers, and software with required software licenses.
- Over-write hard drives before discarding computer equipment.

3. **Network Administration** – Here, the ITD employees manage the organization's technology backbone, i.e., its data servers and networks. They design, implement, and maintain server and network configurations, routing protocols, and storage environments. They monitor usage and loads, and implement programs to minimize system downtime. They coordinate system backup, storage, and retrieval systems. They facilitate the organization-wide design and test of disaster recovery and business continuity plans.

Best Practices:

- Develop network documentation and network change authorization procedures.
- Assign unique ID's for all users, including administrators.
- Institute system redundancies.

- Maintain an inventory of information assets (i.e., data) that classifies the data according to sensitivity and identifies where the data resides.
- Understand applicable laws and regulations surrounding the data (i.e., confidentiality requirements, sunshine laws, etc.).
- Protect inter-facility networks with a Virtual Private Network (VPN) that requires an encrypted connection.
- Consider record retention and Sunshine Law requirements.

Network Access

- Work with departments to establish new user access profiles commensurate with job responsibilities.
- Limit access to dangerous or inappropriate web sites.
- Monitor your systems (establish baselines, watch trends, intrusion detection systems, security incident logs, etc.).

Backups and Contingency Plans

- Backup regularly and test restores. Store backup media off-site (or the cloud).
- Develop a disaster recovery plan and perform training runs.
- Develop a security incident response plan.

4. **Application Installation/Development, Support, and Change Management** – These ITD employees work with end users and customers to develop system needs and specifications. They research, develop/acquire, and install new software for end users. They coordinate software training and support, troubleshoot technical issues, and fine tune applications for users. They implement software updates including bug fixes, patches, enhancements and customized options.

Best Practices:

- Prohibit user software installations (installations done by IT).
- Establish and maintain a relationship with vendor support departments.
- Design Go-Live plans for major software installations.
- Coordinate adequate training on new software.
- Use an automated deployment system and log the timely installation of all software updates, patches, changes, etc.
- Use audit trails to detect unapproved changes.
- Implement change management processes that require authorization and testing.

5. **Business Development** – These ITD employees develop databases and applications that pool, extract, and analyze data for management insight and use. They use tools like SQL databases to manage the organization's data and produce reports.

Best Practices:

- Understand user needs and data characteristics.
- Based on user needs, maximize efficiency through re-use of applicable and supported systems.

6. **Security** – These ITD employees design, communicate, and enforce policies and procedures to mitigate risk from internal and external data breaches and cyberattacks. They remain abreast of changes in rules and regulations pertaining to cybersecurity. They develop and implement security incident management plans. They ensure protection of private data (e.g., bank account information, social security numbers, etc.) when it resides in the organization's systems. Securing data means securing the confidentiality, integrity, and availability of the data. There is a happy medium between security and convenience.

Best Practices:

<u>Physical Controls</u>

- Establish physical controls (guards, gates, cameras, and/or locks, etc.,) in buildings and server rooms.
- Make sure server areas have appropriate environmental protection such as smoke detectors, fire alarms and extinguishers, and uninterrupted power supplies.

<u>Network Security</u>

- Add a firewall between the internet and the network, and ensure it is monitored and updated. Ensure that access to the firewall or router is password protected.
- Employ website filters and scans.
- Utilize a centrally-managed anti-virus system with regular automatic updates.
- Install intrusion prevention systems and/or anti-malware software (e.g., ransomware or multi-factor authentication (MFA)) to minimize system criminal attacks.
- Draft incident management policies and procedures (to prevent an incident from becoming a disaster).

Perform vulnerability scans or penetration testing (or outside security audit). Institute procedures for encrypting proprietary information.

<u>Banking and Customer Interfaces</u>

- Only transfer private data over secure networks, e.g., VPN's with appropriate encryption technology.
- Use wired networks only for banking transactions and online access.
- Use Payee Positive Pay and "dual authorizations" and/or build layered-defense mechanisms for online banking transactions.

- Monitor bank activity daily.
- Carefully check ACH/direct deposit authorization forms and change requests and verify them with authorized vendor representatives by telephone to minimize fraud risk.

Ensure systems are in compliance with banking institution's compliance requirements, including PCI compliance for merchant services.

End Users

- Provide user security education and awareness training.
- Remove/change default passwords.
- Require complex passwords for all users, changed regularly. Consider the need for multifactor authorization.
- Remove access credentials at an employee's termination or transfer.
- Institute relatively short session time-outs.
- Limit/control super user privileges and the use of shared accounts.
- Follow the principle of least privilege where a user's access should be limited to the specific data, resources and applications needed to complete their work.

Perform periodic reviews of user access for segregation of duties conflicts and to ensure user access follows the principle of least privilege.

Ensure the organization's policies and procedures are in compliance with federal, state and local legislation pertaining to cybersecurity including Section 112.22, F.S. (recently created by Laws of Florida Chapter 2023-32), which requires governments to block all prohibited applications on any government-issued devises.

- In Florida, Section 282.318, F.S., also known as the "State Cybersecurity Act", sets forth the standards and processes for assessing state agency cybersecurity risks and determining appropriate security measures.

- Although Section 282.318, F.S., does not specifically apply to local governments, some of the requirements constitute good business practice voluntary measures to mitigate cybersecurity risks.

- Section 282.318, F.S., was amended in 2022 (Laws of Florida Chapter 2022-220 / HB 7055). Key amendments to Section 282.318, F.S., include, but are not limited to, requirements for State agencies to:
  - Report cybersecurity and ransomware incidents.
  - Provide cybersecurity training.
  - Require after-action and other reports.
  - Prohibit certain entities from paying or otherwise complying with ransomware demands.

Security – Defense in Depth

Defense-in-depth refers to the implementation of multiple layers of security to protect data, networks, and systems. Building successive layers of defense mechanisms can reduce the risk of a successful attack by someone with malicious intent. There is no single control that can be used to adequately protect against sophisticated threats. A combination of controls is needed.

Size of the Department

The size of an ITD should be proportional to the size of the organization. The more users and data on the information infrastructure, the more individuals are needed to manage those users and data. In a small organization, one qualified individual may be able to handle all the above responsibilities. Lacking a qualified individual, the organization can retain an outside consultant or utilize managed services, but should do so under a carefully written contract. A benefit of using an outside consulting firm may be access to individuals with varied experiences in the above areas.

Finance Involvement

The organization's finance team should understand the IT operations, whether or not there are IT specialists on the organization's team. A background in IT is not necessary to ask questions about key IT internal controls and understand the answers. Extensive IT knowledge is not necessary to perform extensive procedures (e.g., review documents or reports) that can corroborate these answers. The finance team should work with IT to develop and fully test all financial reports. An evaluation of the financial software systems should be a component of the annual external audit.

Federal and State Resources for Information Technology

The State of Florida Digital Service (FL [DS]) was established in 2020 to help state government deliver better services and improve transparency through design and technology. FL [DS] is the lead entity responsible for establishing standards and processes for assessing state agency cybersecurity risks and determining appropriate security measures. The FL [DS] website features useful information pertaining to cybersecurity, such as a Local Government Cybersecurity Resource Packet, and information on Cybersecurity grants and cybersecurity incident response.

The Cybersecurity & Infrastructure Security Agency (CISA) is the is the operational lead for Federal cybersecurity and the national coordinator for critical infrastructure security and resilience. Through the Infrastructure Investment and Jobs Act of 2021, Congress established the State and Local Cybersecurity Improvement Act, which established the State and Local Cybersecurity Grant Program. CISA is the program management subject-expert in cybersecurity related issues. The CISA website provides resources to local governments on the State and Local Cybersecurity Grant Program.

References

Florida League of Cities:
https://floridaleagueofcities.com/social-media

Florida Local Government Information Systems Association:
http://www.flgisa.org

Free Cyber Self-Assessment Checklist:
https://www.glatfelterpublicentities.com/Portals/0/Cyber-Self-Assessment.pdf

Manual – IT Governance and organization self-assessment:
http://www.osc.state.ny.us/localgov/pubs/lgmg/itgovernance.pdf

Security Training:
https://www.cisecurity.org/

Florida Digital Service (FL[DS]):
https://digital.fl.gov/about/

Cybersecurity & Infrastructure Security Agency (CISA):
https://www.cisa.gov/

CISA State and Local Cybersecurity Grant Program:
https://www.cisa.gov/state-and-local-cybersecurity-grant-program