SECTION 23 – INFORMATION TECHNOLOGY

Overview

Information Technology (IT) involves the use of computer systems, hardware, software, and networks to create, store, secure, process, and exchange data and information. 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 spreadsheets, and report to governing bodies with presentation software.

Employees use email, telephones, mobile devices, communication platforms (e.g., Zoom, Teams), and the internet for communications. 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, 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funding for the maintenance of hardware, software, and the computer network, the organization risks: (1) becoming outdated; (2) data loss due to hardware failure; and (3) suffering from lack of interoperability between departments and other agencies.

Local Government Cybersecurity Requirements

Section 282.3185, Florida Statutes, applies to counties and municipalities and requires cybersecurity standards consistent with generally accepted best practices, including the National Institute of Standards and Technology Cybersecurity Framework.

Employees with network access must complete basic cybersecurity training within 30 days after commencing employment and annually thereafter. Technology professionals and employees with access to highly sensitive information must complete advanced training on the same schedule.

Counties and municipalities must maintain written procedures for cybersecurity and ransomware incident notification. Severity level 3, 4, or 5 cybersecurity incidents must be reported to the Cybersecurity Operations Center, the Cybercrime Office of the Florida Department of Law Enforcement, and the sheriff having jurisdiction as soon as possible but no later than 48 hours after discovery; ransomware incidents must be reported no later than 12 hours after discovery. A local government must submit an after-action report to the Florida Digital Service within one week after remediation. Coordinate any applicable breach notice under Section 501.171, Florida Statutes. Cybersecurity records and meetings may be protected as provided in Section 119.0725, Florida Statutes.

Under Section 282.3186, Florida Statutes, a county or municipality experiencing a ransomware incident may not pay or otherwise comply with a ransom demand.

Responsibilities of the Department

IT 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 leads the organization's technology program, including infrastructure, applications, cybersecurity, data, personnel, vendors, budgets, and major projects. The IT leader aligns technology priorities with organizational goals, establishes policies and performance expectations, manages risk, and recommends investments that improve service delivery, security, resilience, and efficiency. They also keep executive leadership informed of significant needs, costs, risks, and decisions, supporting the mission and responsible use of public funds.

    a) Best Practices

        i) Maintain a strong working relationship with the chief executive and leadership team. Provide concise, regular updates on service performance, projects, cybersecurity risks, spending, staffing needs, and decisions requiring executive support.

        ii) Stay current through professional associations, government technology groups, conferences, training, official security advisories, and reputable publications. Evaluate new technologies based on business value, maturity, security, supportability, and total lifecycle cost.

        iii) Learn from other public agencies and established industry frameworks. Reuse proven standards, contracts, templates, and lessons learned when practical, while adapting them to local legal, operational, security, and budget requirements.

        iv) Establish a cross-departmental technology steering group to gather feedback, review initiatives, prioritize competing requests, and communicate major changes. Consult legal counsel to determine whether the group is subject to Florida's Government-in-the-Sunshine Law.

        v) Work with departments to identify critical business processes, dependencies, and acceptable downtime. Prioritize projects and investments based on public impact, legal deadlines, financial exposure, data sensitivity, operational risk, and available resources.

2) **IT Hardware and Software Procurement –** IT staff manage the lifecycle of hardware, software, cloud services, subscriptions, and professional services, from requirements and acquisition through support, replacement, and secure disposal. They coordinate with departments, Procurement, Finance, Legal, and Security to evaluate compatibility, accessibility, licensing, support, privacy, cybersecurity, and total lifecycle cost, not just purchase price.

    a) Best Practices

        i) Acquire technology only for a documented business or operational need. Before selection, define expected outcomes, responsible owner, dependencies, security, privacy, accessibility, data ownership and return, retention, support, exit needs, and total lifecycle cost.

ii) Standardize approved hardware, software, configurations, upgrades, and support options when practical. Standardization improves compatibility, security, patching, training, support, reuse, and purchasing leverage. Document and approve legitimate exceptions.

iii) Coordinate technology purchasing through IT and Procurement, including cloud services and department-funded solutions. Departments define business needs, IT validates technical and security requirements, and Procurement ensures compliance with purchasing and competitive selection rules.

iv) Maintain current inventories for hardware, software, subscriptions, and licenses. Track asset and serial numbers, ownership, assignment, location, configuration, purchase and lifecycle dates, warranty or support status, renewal dates, costs, license entitlements, and final disposition. Reconcile records periodically.

v) Before equipment is reused, transferred, surplused, or disposed of, confirm that required records have been retained, transferred, or authorized for disposition. Sanitize or destroy storage media using an approved, documented method appropriate to the media and data sensitivity. Retain required chain-of-custody and disposition records, and apply FBI CJIS Security Policy requirements to media containing criminal justice information (CJI).

3) **IT Infrastructure and Network Operations –** ITD staff oversee the core technology systems and connectivity that keep the organization operating, including servers, storage, cloud services, networks, firewalls, remote access, and connections between facilities. They design, secure, monitor, maintain, and upgrade the environment; manage capacity, availability, configurations, incidents, and vendor support; and minimize service disruptions. They also coordinate backup and recovery, support disaster recovery, and business continuity planning with business owners, Security, Emergency Management, and leadership.

a) Best Practices

i) Maintain current diagrams, inventories, configurations, IP ranges, circuits, dependencies, support contacts, and recovery procedures. Use formal change controls that include risk review, approval, testing, communication, rollback planning, and post-change validation.

ii) Assign unique accounts or identifiers to users, administrators, service accounts, and system processes. Use separate standard and privileged administrator accounts, avoid shared accounts, require multifactor authentication for privileged and remote user access, enforce least privilege, disable inactive accounts, and retain traceable logs.

iii) Provide redundancy based on each service's criticality and outage impact. Reduce single points of failure across equipment, power, network paths, internet connections, storage, and facilities, and regularly test failover. Backups do not replace operational redundancy.

iv) Working with data owners, records management, and security, maintain an information asset inventory showing ownership, sensitivity, location, data flows, authorized users, third-party access, retention requirements, and safeguards. Update it when systems, vendors, integrations, or processes change.

v) Identify legal, regulatory, contractual, and policy requirements for systems and data, including privacy, breach notification, public records, retention, and the FBI Criminal Justice Information Services (CJIS) Security Policy when systems store, process, or transmit criminal justice information (CJI). Coordinate controls with Legal, Security, Privacy, Records Management, and affected departments.

vi) Encrypt inter-facility communications that cross public, shared, or untrusted networks using a properly configured site-to-site VPN or equivalent. Apply strong authentication, secure protocols, key management, monitoring, segmentation, and firewall controls based on risk.

vii) Build public-records, legal-hold, and retention requirements into technology systems. Preserve records subject to an audit, litigation, or pending public-records request, and document authorized disposition under applicable state schedules. Do not rely on operational backups as the official records repository.

b) Network Access

i) Work with departments to establish new user access profiles commensurate with job responsibilities.

ii) Limit access to dangerous or inappropriate websites.

iii) Monitor your systems (establish baselines, watch trends, intrusion detection systems, security incident logs, etc.).

c) Backups and Contingency Plans

i) Backup regularly and test restores. Store backup media off-site (or the cloud).

ii) Develop a disaster recovery plan and perform training runs.

iii) Develop a security incident response plan

4) **Application Installation/Development, Support, and Change Management –** These IT 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.

a) Best Practices
i) Prohibit user software installations (installations done by IT).
ii) Establish and maintain a relationship with vendor support departments.
iii) Design Go-Live plans for major software installations.
iv) Coordinate adequate training on new software.
v) Use an automated deployment system and log the timely installation of all software updates, patches, changes, etc.
vi) Use audit trails to detect unapproved changes.
vii) 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.

a) Best Practices
i) Understand user needs and data characteristics.
ii) 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) 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.

a) Best Practices
i) Physical Controls
(1) Establish physical controls (guards, gates, cameras, and/or locks, etc.,) in buildings and server rooms.
(2) Make sure server areas have appropriate environmental protection such as smoke detectors, fire alarms and extinguishers, temperature control, and uninterrupted power supplies.

ii) Network Security
   (1) 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.
   (2) Employ website filters and scans.
   (3) Utilize a centrally-managed anti-virus system with regular automatic updates.
   (4) Deploy appropriately managed intrusion-detection or prevention, endpoint-protection, anti-malware, and ransomware controls. Require multifactor authentication for privileged, remote, and other high-risk access.
   (5) Develop, maintain, and test incident-response and continuity procedures so that security events are identified, contained, communicated, recovered from, and documented.
   (6) Conduct vulnerability scanning, penetration testing, or independent security assessments based on risk. Encrypt confidential and sensitive information in transit and at rest when appropriate.

iii) Banking and Customer Interfaces
   (1) Transmit confidential or sensitive data only through managed, encrypted connections, such as appropriately configured VPNs or secure web services.
   (2) Use trusted, managed devices and networks for banking and other sensitive transactions and avoid public or unsecured wireless networks.
   (3) Use payee positive pay, dual authorization, and out-of-band verification or other layered controls for online banking and payment transactions.
   (4) Monitor bank activity daily.
   (5) Carefully check ACH/direct deposit authorization forms and change requests and verify them with authorized vendor representatives by telephone to minimize fraud risk.
   (6) Ensure systems are in compliance with banking institution's compliance requirements, including PCI compliance for merchant services.

iv) End Users
   (1) Provide user security education and awareness training regularly.
   (2) Remove/change default passwords.
   (3) Require long passwords or passphrases, screen new passwords against lists of common or compromised values, and use multifactor authentication for high-risk access. Do not require routine password changes unless there is evidence of compromise. (See NIST SP 800-63B, Section 3.1.1.2.)
   (4) Remove access credentials at an employee's termination or transfer.
   (5) Configure risk-based session time-outs and reauthentication requirements, particularly for privileged or sensitive systems.
   (6) Limit/control super user and system administrator privileges, and the use of shared accounts.
   (7) 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.
   (8) Perform periodic reviews of user access for segregation of duties conflicts and to ensure user access follows the principle of least privilege.

7) **Artificial Intelligence and Emerging Technology –** IT, Finance, Legal, Security, Records Management, and business owners should establish governance for artificial intelligence (AI), including generative AI and AI features embedded in enterprise software. Governance should address approved uses, data handling, vendor risk, human oversight, records retention, security, and accountability.

   a) Best Practices

      i) Maintain an inventory of approved AI tools and AI-enabled systems and establish a review process for new uses. Address unauthorized or "shadow AI" through policy, training, technical controls, and procurement oversight.

ii) Classify AI use cases based on data sensitivity, degree of automation, potential financial or legal impact, and consequences to individuals. Require increased Security, Legal, Privacy, Records Management, or executive review as risk increases.

iii) Do not enter confidential, exempt, sensitive, protected, or otherwise restricted government information into public or external AI services unless the use has been specifically authorized and appropriate contractual, privacy, security, and records controls are in place. Apply Chapter 119, Florida Statutes, and applicable retention requirements to AI inputs and outputs as appropriate.

iv) Require meaningful human review for AI-assisted outputs that could materially affect financial decisions, eligibility, personnel actions, enforcement, legal rights, public communications, or other high-impact governmental decisions.

v) For third-party AI products, address data ownership, model training, retention and deletion, security, auditability, subprocessors, intellectual-property rights, public-records obligations, and the return or destruction of government data at termination.

vi) Use established risk-management resources, such as the NIST Artificial Intelligence Risk Management Framework (AI RMF) and the NIST Generative Artificial Intelligence Profile, when developing AI governance and controls.

Ensure that the organization's policies and procedures comply with applicable federal, state, and local cybersecurity requirements, including Section 112.22, Florida Statutes, which requires governmental entities to block prohibited applications on government-issued devices and networks as specified by law.

Section 282.318, Florida Statutes, governs state-agency cybersecurity. Counties and municipalities are governed by the Local Government Cybersecurity Act, Section 282.3185, Florida Statutes, including its cybersecurity-training and incident-reporting requirements. Covered employees must complete the applicable training within 30 days after commencing employment and annually thereafter.

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.

Financial Systems Access Controls and Segregation of Duties

Automated financial systems require access controls that protect system integrity and support sound internal control. Finance and IT or the applicable system administrator should coordinate user provisioning, role design, privileged access, segregation of duties, and periodic review.

- Grant access based on documented job responsibilities, role-based access, and least privilege. Approval authority should be assigned by an appropriate department official or system owner.
- Separate transaction initiation from approval when practicable. When staffing or system limitations prevent full segregation, document and monitor compensating controls.
- Promptly deactivate access when an employee terminates; remove prior-department approval authority when an employee transfers; and revise security and workflow roles when duties change. Local procedures should define responsibility and notification methods for these changes.
- Perform documented periodic reviews of financial-system access, segregation-of-duties conflicts, privileged or super-user access, and workflow authority. Finance, IT/system administrators, and business owners should resolve inappropriate or obsolete access and retain evidence of the review.

Payment Security (PCI DSS)

Governments that accept payment cards should maintain controls consistent with the current Payment Card Industry Data Security Standard (PCI DSS) and the requirements of their acquiring bank, payment brands, and service providers.

- Minimize the storage and handling of cardholder data. Mask primary account numbers (PAN) when displayed unless a legitimate business need requires additional digits, and do not store sensitive authentication data such as card verification codes or PIN/PIN blocks after authorization.
- Maintain an inventory of payment channels, point-of-sale devices, gateways, integrations, and third-party service providers that can affect payment security or PCI scope.
- Obtain and review current PCI DSS validation evidence appropriate to third-party payment providers, such as an Attestation of Compliance when applicable, at least annually and when significant changes occur. Do not treat vendor outsourcing as eliminating the government's responsibility to understand shared controls.
- Define payment-security responsibilities in contracts and service agreements, including incident notification, data retention and deletion, integration security, service availability, and responsibility for maintaining applicable PCI DSS compliance.

Cloud and Third-Party Vendor Risk Management

Cloud and third-party services can create operational, financial, cybersecurity, records-management, and data continuity risks. Critical vendors should be evaluated throughout the contract lifecycle, not only at purchase.

- Before acquisition, assess vendor security, privacy, financial viability, service availability, data location and handling, subcontractors, business continuity, incident response, and ability to meet legal and records requirements.
- Use contracts and service-level agreements to define data ownership, access, export format, return or deletion at termination, retention, recovery objectives, uptime and support expectations, breach and incident notification, audit rights, and transition assistance.
- For critical hosted systems, periodically review relevant security and compliance reports, service performance, incidents, vulnerabilities, insurance or risk-transfer requirements, and significant changes in the vendor's environment.
- Use a documented offboarding process that addresses data export, records retention, user and administrator accounts, keys and tokens, interfaces, payment credentials, licenses and renewals, equipment return, and confirmation of secure data deletion or media sanitization.

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 key IT operations and controls, whether technology functions are performed internally or by service providers. Finance personnel should ask informed questions, review supporting documentation and reports, and work with IT to develop and test financial reports and interfaces. IT

risks and controls should be considered in the organization's risk assessment and in internal and external audit planning, as applicable. Finance should also participate, as appropriate, in financial-system access reviews, payment-security oversight, third-party technology risk assessment, cyber-incident fiscal impact analysis, and governance of AI used in financial or administrative processes.

Federal and State Resources for Information Technology

Florida Digital Service. The Florida Digital Service was established to improve state technology services and cybersecurity. It provides standards, guidance, training, incident-reporting information, and resources that may assist state and local governments.

The Florida Digital Service is the lead state entity for specified cybersecurity responsibilities. Its website includes local-government cybersecurity resources, training information, grant information when available, and incident-response guidance.

Section 282.31855, Florida Statutes, creates the Local Government Cybersecurity Protection Program within the Florida Digital Service. The program provides eligible local governments with cybersecurity commodities and services to develop and enhance cybersecurity risk-management programs and defend against threats, including ransomware. Statutory awards are made by December 1 of each year under the program criteria, with preference given to fiscally constrained counties.

The Cybersecurity and Infrastructure Security Agency (CISA) is a U.S. Department of Homeland Security agency responsible for reducing cyber and physical risk to critical infrastructure. CISA works with public- and private-sector partners to identify and manage risk and to strengthen resilience.

CISA offers free cybersecurity services, assessments, alerts, and tools to public-sector organizations. Federal and state grant opportunities may also be available periodically; governments should verify current eligibility, application periods, and award requirements through official sources.

References

- Section 112.22, Florida Statutes - Use of prohibited applications on government-issued devices. Official link
- Section 119.0725, Florida Statutes - Cybersecurity public records and public meetings exemptions. Official link
- Section 282.3185, Florida Statutes - Local Government Cybersecurity Act. Official link
- Section 282.31855, Florida Statutes - Local Government Cybersecurity Protection Program. Official link
- Section 282.3186, Florida Statutes - Ransomware incident compliance. Official link
- Section 501.171, Florida Statutes - Security of confidential personal information and breach notification. Official link
- Florida Digital Service - Cybersecurity resources. Official link
- National Institute of Standards and Technology - Cybersecurity Framework. Official link
- National Institute of Standards and Technology - Special Publication 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management, Section 3.1.1.2, Password Verifiers. Official link
- Cybersecurity and Infrastructure Security Agency - Cybersecurity resources for government. Official link
- Internal Revenue Service - Publication 1075, Tax Information Security Guidelines. Official link
- Florida Local Government Information Systems Association. Official link
- Section 119.071, Florida Statutes - General exemptions from inspection or copying of public records. Official link
- National Institute of Standards and Technology - Artificial Intelligence Risk Management Framework (AI RMF 1.0). Official link
- National Institute of Standards and Technology - Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST AI 600-1). Official link
- National Institute of Standards and Technology - Special Publication 800-88 Rev. 2, Guidelines for Media Sanitization. Official link
- PCI Security Standards Council - Payment Card Industry Data Security Standard (PCI DSS) v4.0.1. Official link