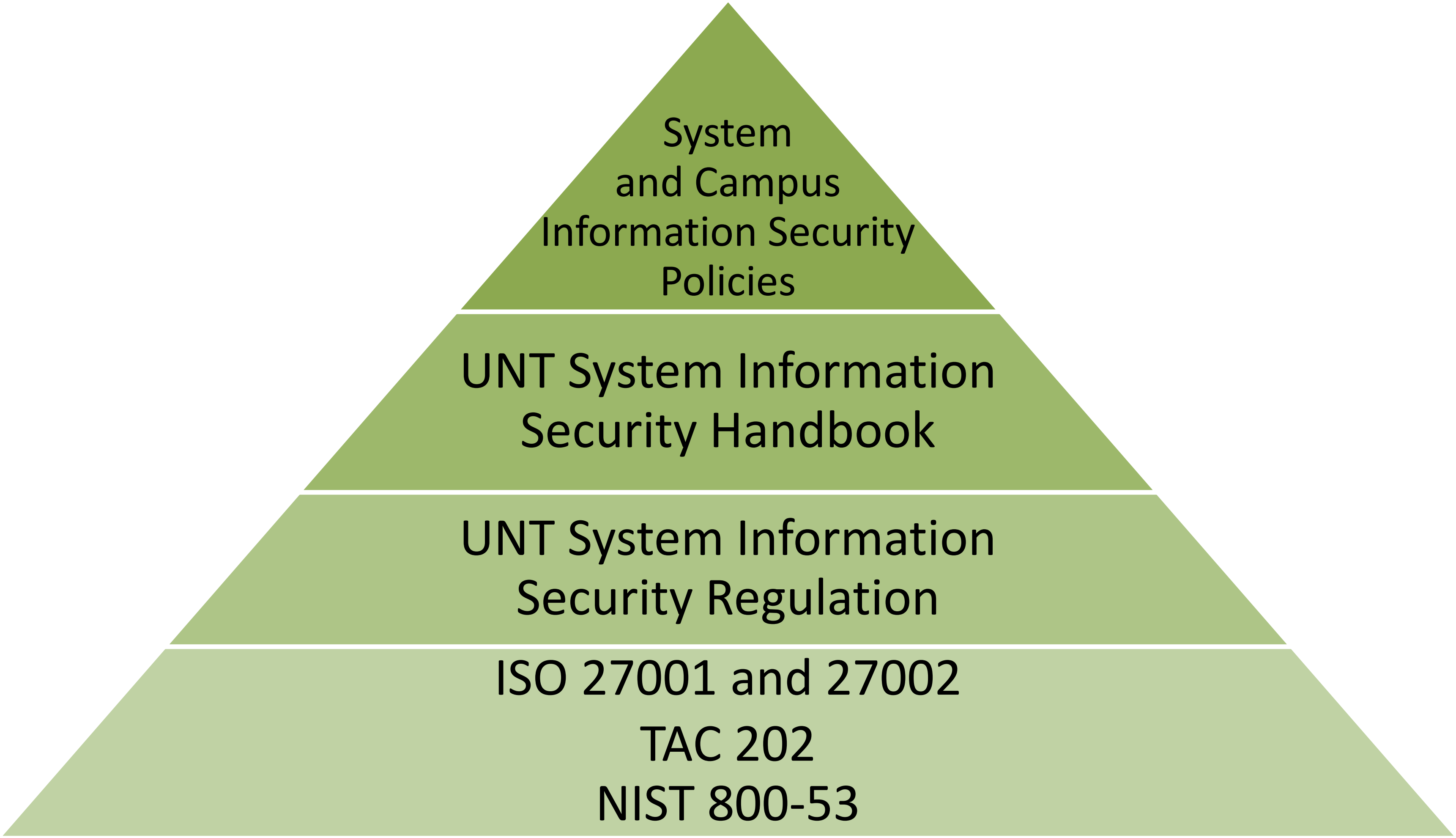
Information Security Policy and Handbook Overview

UNT SYSTEM
IT SHARED SERVICES

ITSS Information Security

June 2015

Information Security Policy Control Hierarchy



System and Campus Information Security Policies

UNT System Information Security Handbook

UNT System Information Security Regulation

ISO 27001 and 27002

TAC 202

NIST 800-53

Information Security Program Documents

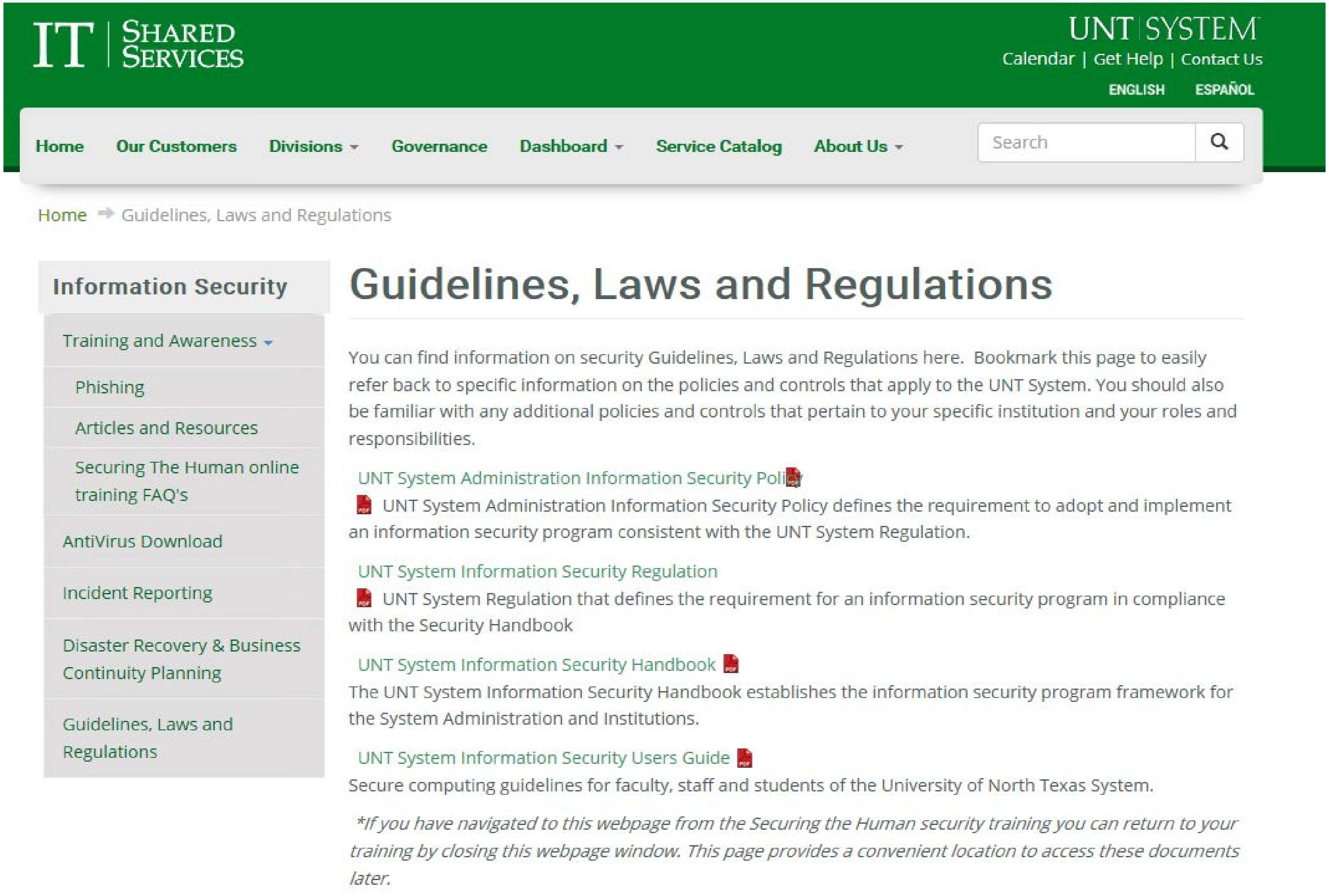
UNT System Information Security Policy

- Requires the adoption and implementation of a security program
- Requires any security program to be consistent with the UNT System Information Security Handbook

UNT System Information Security Handbook

- Establishes the security program framework
- Is based on 1TAC 202 and 203, and ISO 27001 and 27002
- Applies to all users of information and information resources of UNT System and Institutions

https://itss.untsystem.edu/security/guidelines-laws-and-regulations



Guidelines, Laws and Regulations

You can find information on security Guidelines, Laws and Regulations here. Bookmark this page to easily refer back to specific information on the policies and controls that apply to the UNT System. You should also be familiar with any additional policies and controls that pertain to your specific institution and your roles and responsibilities.

UNT System Administration Information Security Poli

UNT System Administration Information Security Policy defines the requirement to adopt and implement an information security program consistent with the UNT System Regulation.

UNT System Information Security Regulation

UNT System Regulation that defines the requirement for an information security program in compliance with the Security Handbook

UNT System Information Security Handbook

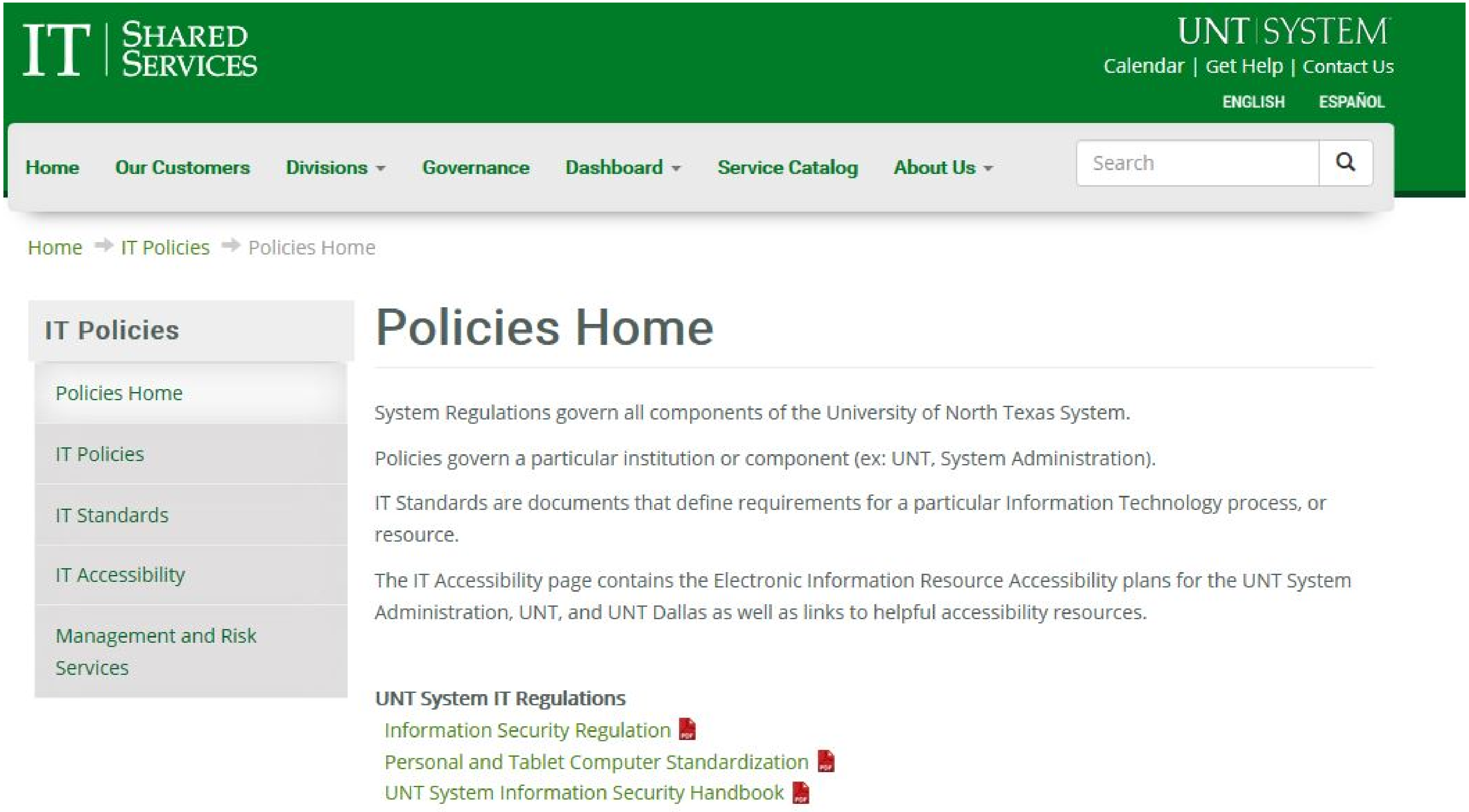
The UNT System Information Security Handbook establishes the information security program framework for the System Administration and Institutions.

UNT System Information Security Users Guide

Secure computing guidelines for faculty, staff and students of the University of North Texas System.

**If you have navigated to this webpage from the Securing the Human security training you can return to your training by closing this webpage window. This page provides a convenient location to access these documents later.*

https://itss.untsystem.edu/it-policies



Policies Home

System Regulations govern all components of the University of North Texas System.

Policies govern a particular institution or component (ex: UNT, System Administration).

IT Standards are documents that define requirements for a particular Information Technology process, or resource.

The IT Accessibility page contains the Electronic Information Resource Accessibility plans for the UNT System Administration, UNT, and UNT Dallas as well as links to helpful accessibility resources.

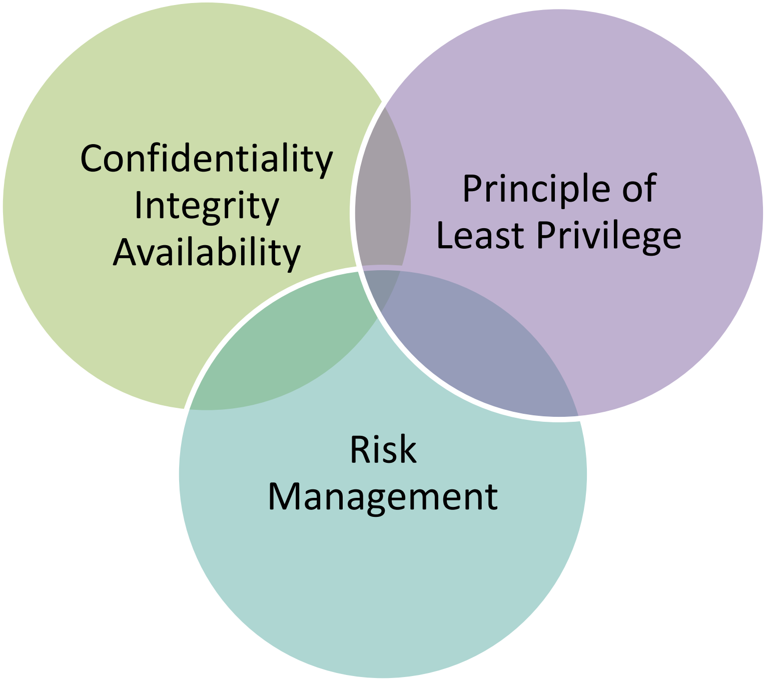
UNT System IT Regulations

- Information Security Regulation
- Personal and Tablet Computer Standardization
- UNT System Information Security Handbook

Policy: Procedures and Responsibilities	Handbook
1. Security Program and Controls	Section 3 Structure of the Handbook Section 5 Information Security Policy Section 15 Compliance with Legal Requirements
2. Information Security Roles	Section 6 Information Security Structure
3. Secure Access and Management of Info Resources	Section 4 Risk Management and Assessment Section 7 Asset Management Section 8 Human Resources Security Section 9 Physical Security Section 10 Communications and Operations Management Section 11 Access Control Section 12 Information Systems Acquisition and Development, Testing and Maintenance
4. Security Incident Management	Section 13 Information Security Incident Management
5. Business Continuity Planning	Section 14 Business Continuity Management
6. Security Exceptions	Section 16 Security Exceptions
7. Sanctions	Section 17 Sanctions for Violations

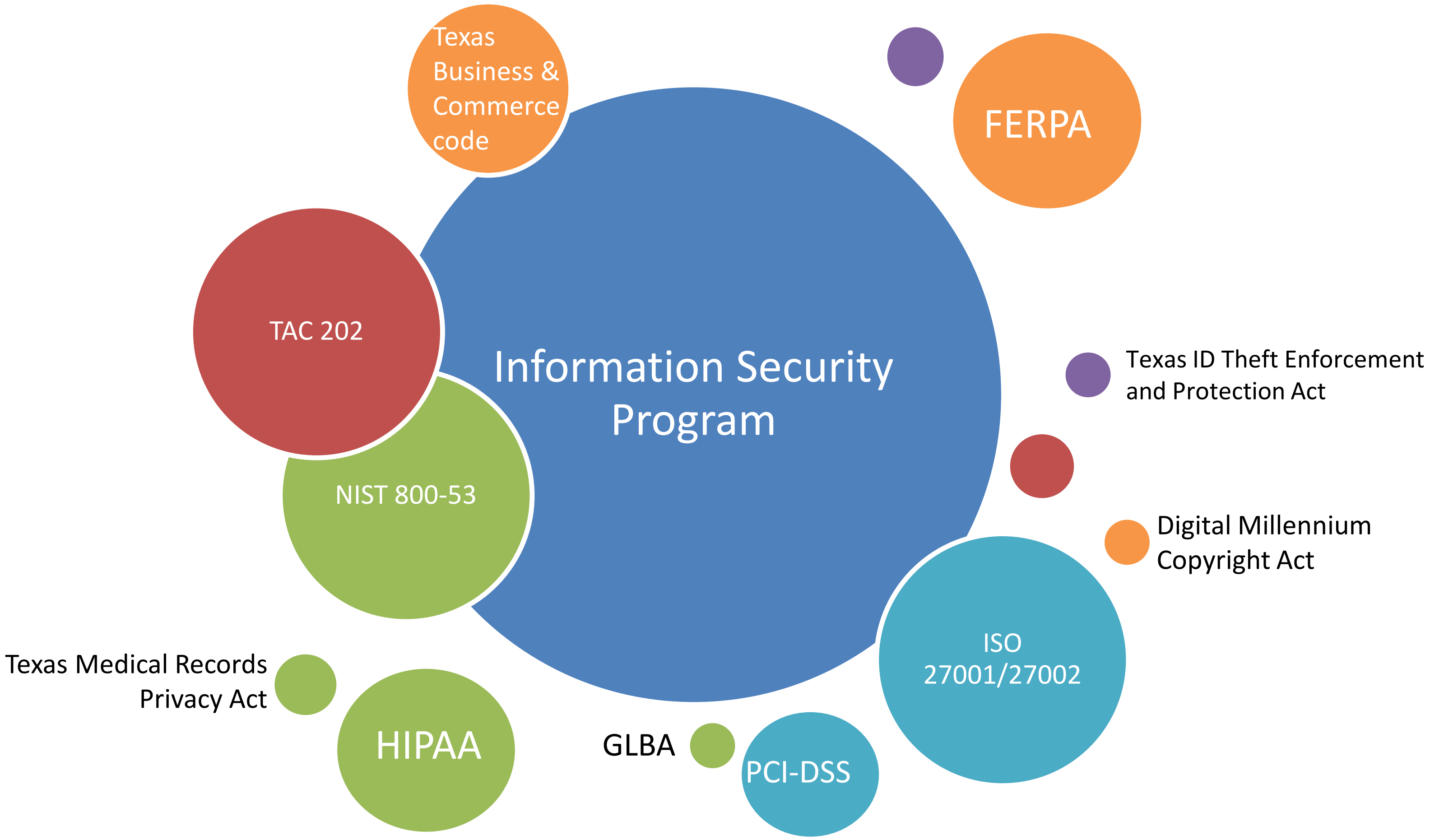
Information Security Handbook

Establishes the information security program framework



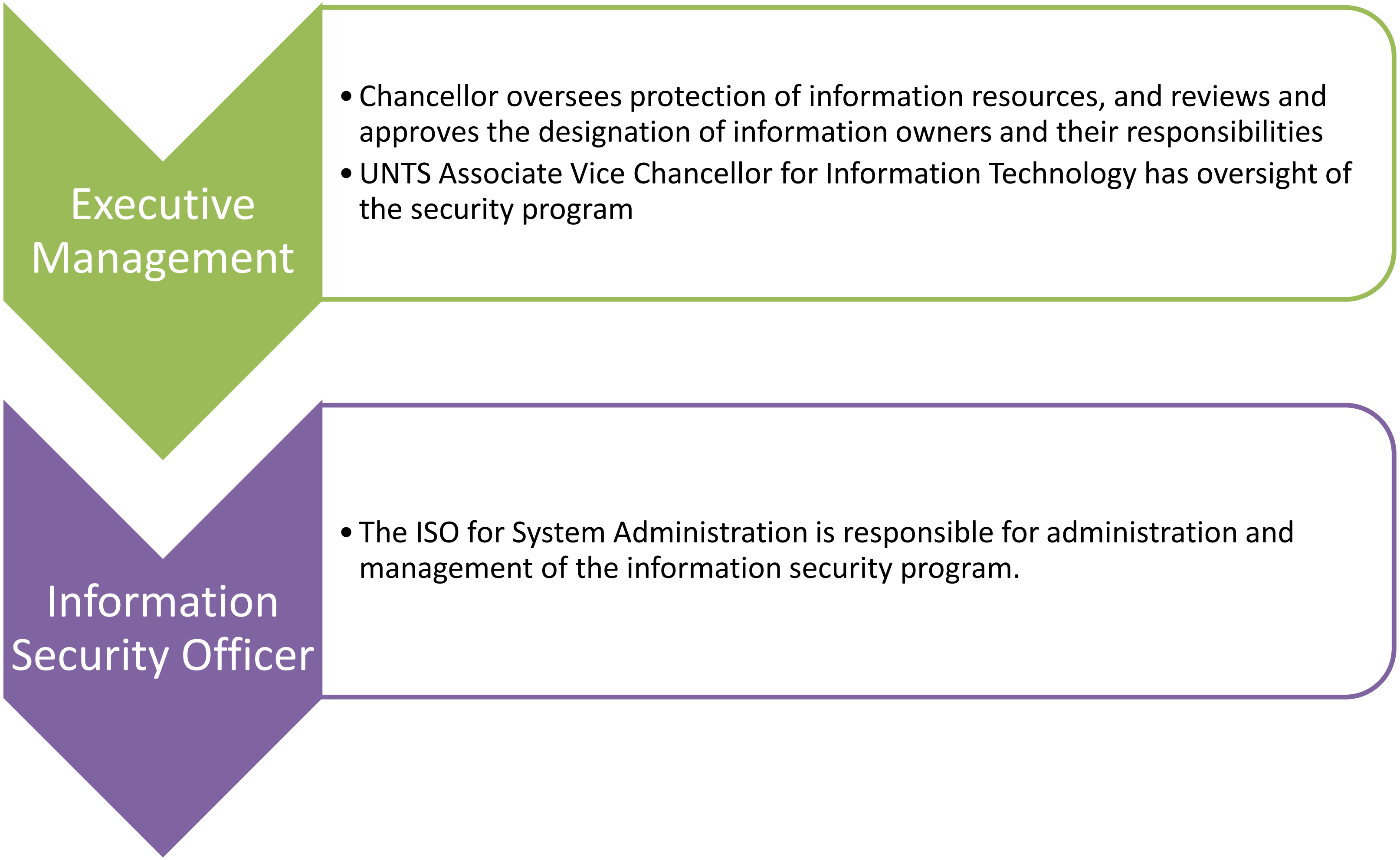
1. Security Program and Controls

Handbook sections 3,5,15


Texas Business & Commerce code
FERPA
Information Security Program
TAC 202
Texas ID Theft Enforcement and Protection Act
NIST 800-53
Digital Millennium Copyright Act
ISO 27001/27002
Texas Medical Records Privacy Act
HIPAA
GLBA
PCI-DSS

2. Roles and Responsibilities

Handbook 6



Executive Management

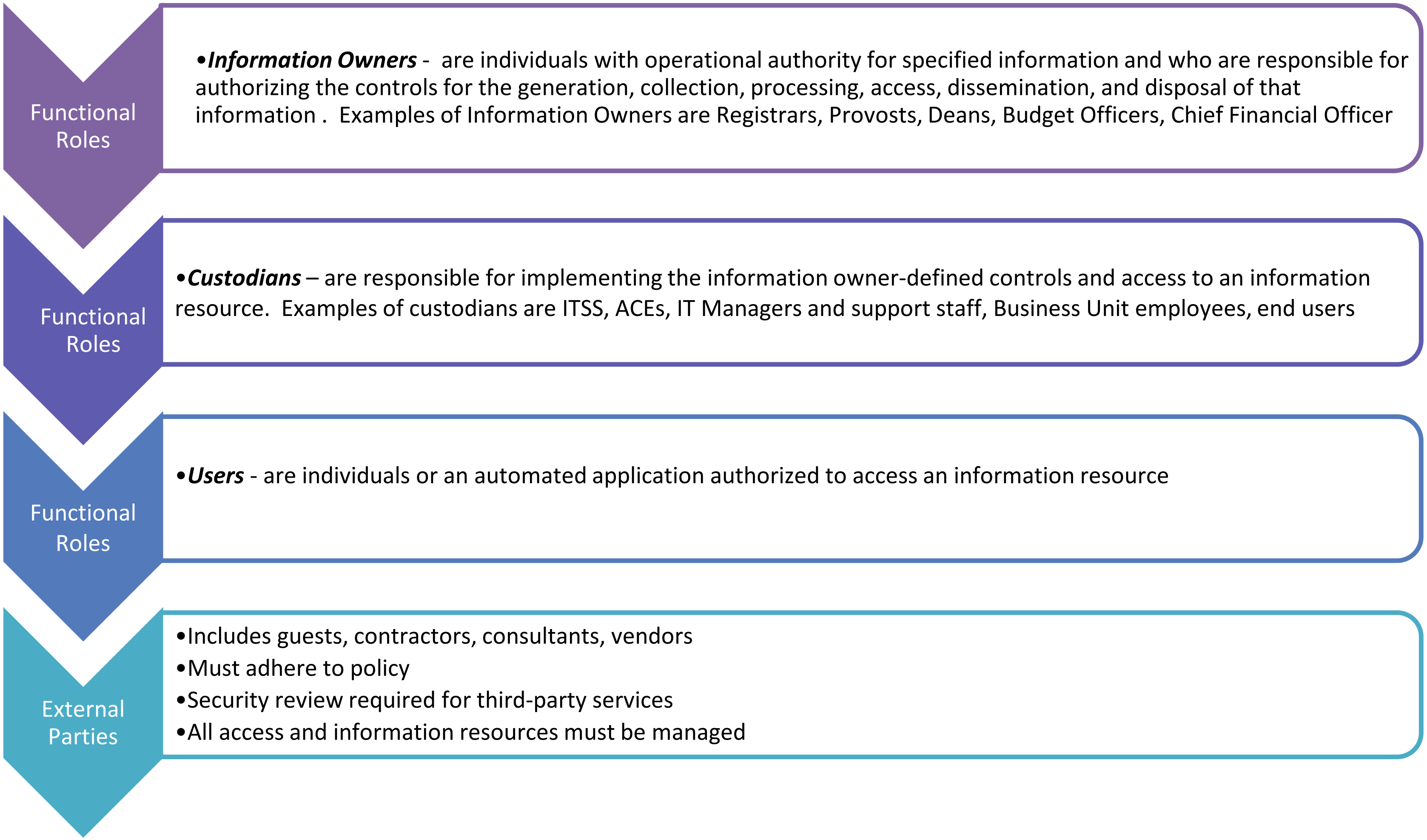
- Chancellor oversees protection of information resources, and reviews and approves the designation of information owners and their responsibilities
- UNTS Associate Vice Chancellor for Information Technology has oversight of the security program

Information Security Officer

- The ISO for System Administration is responsible for administration and management of the information security program.

2. Roles and Responsibilities

Handbook 6



Functional Roles

- ***Information Owners*** - are individuals with operational authority for specified information and who are responsible for authorizing the controls for the generation, collection, processing, access, dissemination, and disposal of that information . Examples of Information Owners are Registrars, Provosts, Deans, Budget Officers, Chief Financial Officer

Functional Roles

- ***Custodians*** – are responsible for implementing the information owner-defined controls and access to an information resource. Examples of custodians are ITSS, ACEs, IT Managers and support staff, Business Unit employees, end users

Functional Roles

- ***Users*** - are individuals or an automated application authorized to access an information resource

External Parties

- Includes guests, contractors, consultants, vendors
- Must adhere to policy
- Security review required for third-party services
- All access and information resources must be managed

2. Roles and Responsibilities

Handbook 6

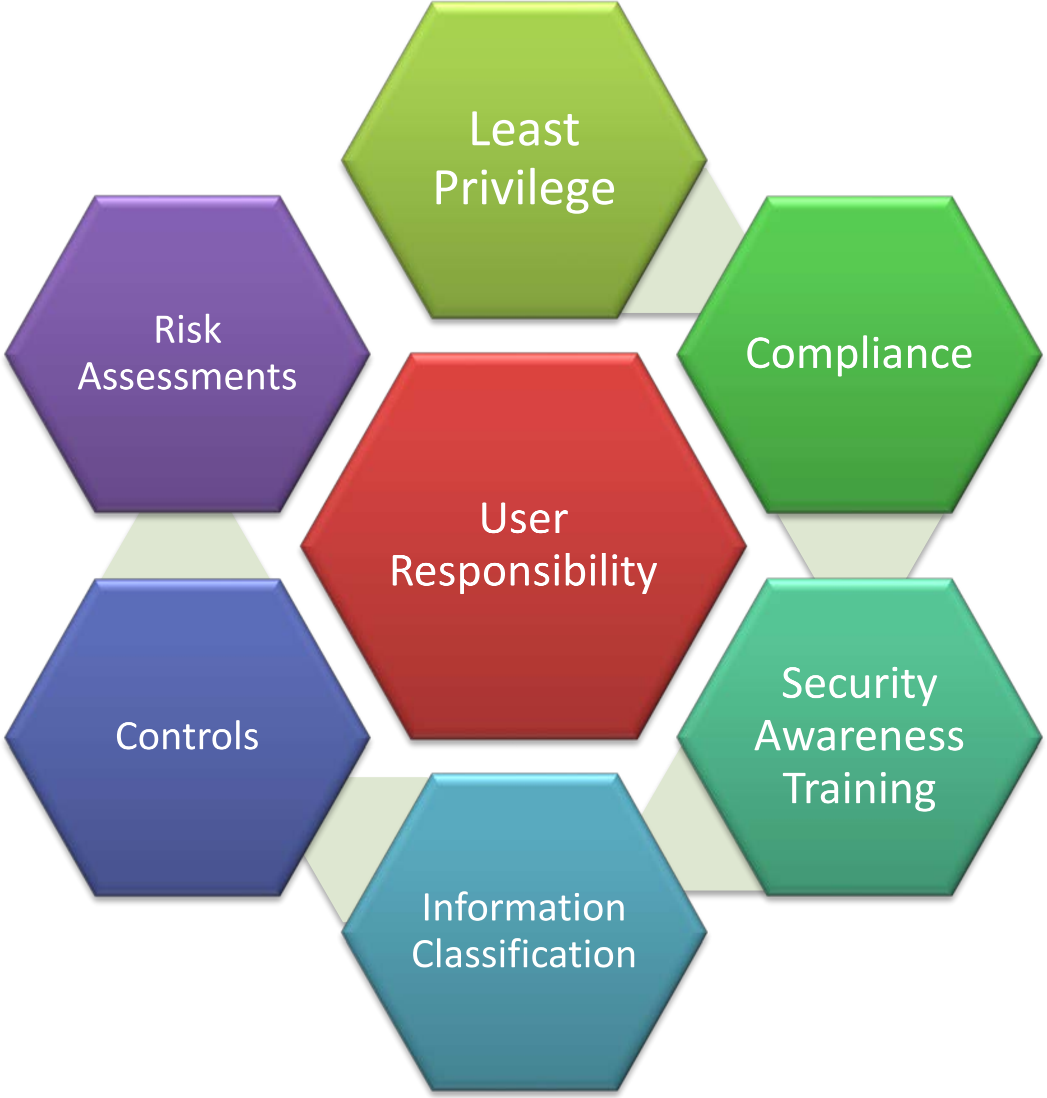
Categories of Information

Category I – Confidential information: e.g. social security numbers, credit card information, student education records.

Category II – Should be controlled before release: e.g. some student directory Information

Category III – Public information available for release.

3. Secure Access and Management of Information



3. Secure Access and Management of Information

Handbook 4

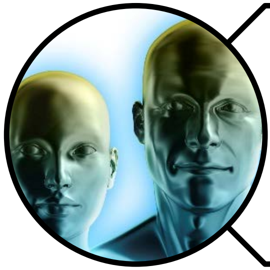
Risk Management

- Risks must be managed (eliminated, mitigated, or accepted).
- The expense of safeguards must be commensurate with the value of information and information resources.
- Institutional management is responsible for risk management decisions

3. Secure Access and Management of Information

Handbook 7,8,9

Asset Management – a documented asset inventory must be maintained. An asset is anything of value to an organization including hardware, software and information



Human Resources Security - Annual Security Awareness training is required for all faculty and staff

Physical Security - Areas housing critical information must be secured physically

3. Secure Access and Management of Information

Handbook 10

Communications and Operations Management

Operational Procedures and Responsibilities

- Principle of Least Privilege
- Separation of Functions
- Password Management
- Manage and monitor networks
- Protect from malicious or unauthorized code

System Planning and Acceptance

- 3rd party agreements require:
  - security review before signing
  - annual compliance review

Protection against Malware, malicious or unwanted programs

- Anti-virus must be used, kept current and not to be disabled by users
- Periodic scans are required

Back-ups

- Required to regularly back up and test mission critical information

3. Secure Access and Management of Information

Handbook 10

Communications and Operations Management

Network Security Management

- Principle of Least Privilege
- Restricted access
- Access must be logged and networks monitored
- Security controls based on criticality and value of the network resources

Media Handling

- Removable media requires encryption and must be securely disposed of

Exchange of Information

- Information exchanged internally and externally must be protected

Electronic Commerce

- Must adhere to PCI DSS

Monitoring

- Must proved a sufficiently complete history of transactions
- Specifies logon banner requirements

3. Secure Access and Management of Information

Handbook 11

Access Control

- User Access Management
- User Responsibility
- Network Access Control
- Operating System Access
- Applications and Information Access
- Mobile computing and telework

Access should be granted and used on the principle of least privilege.

3. Secure Access and Management of Information

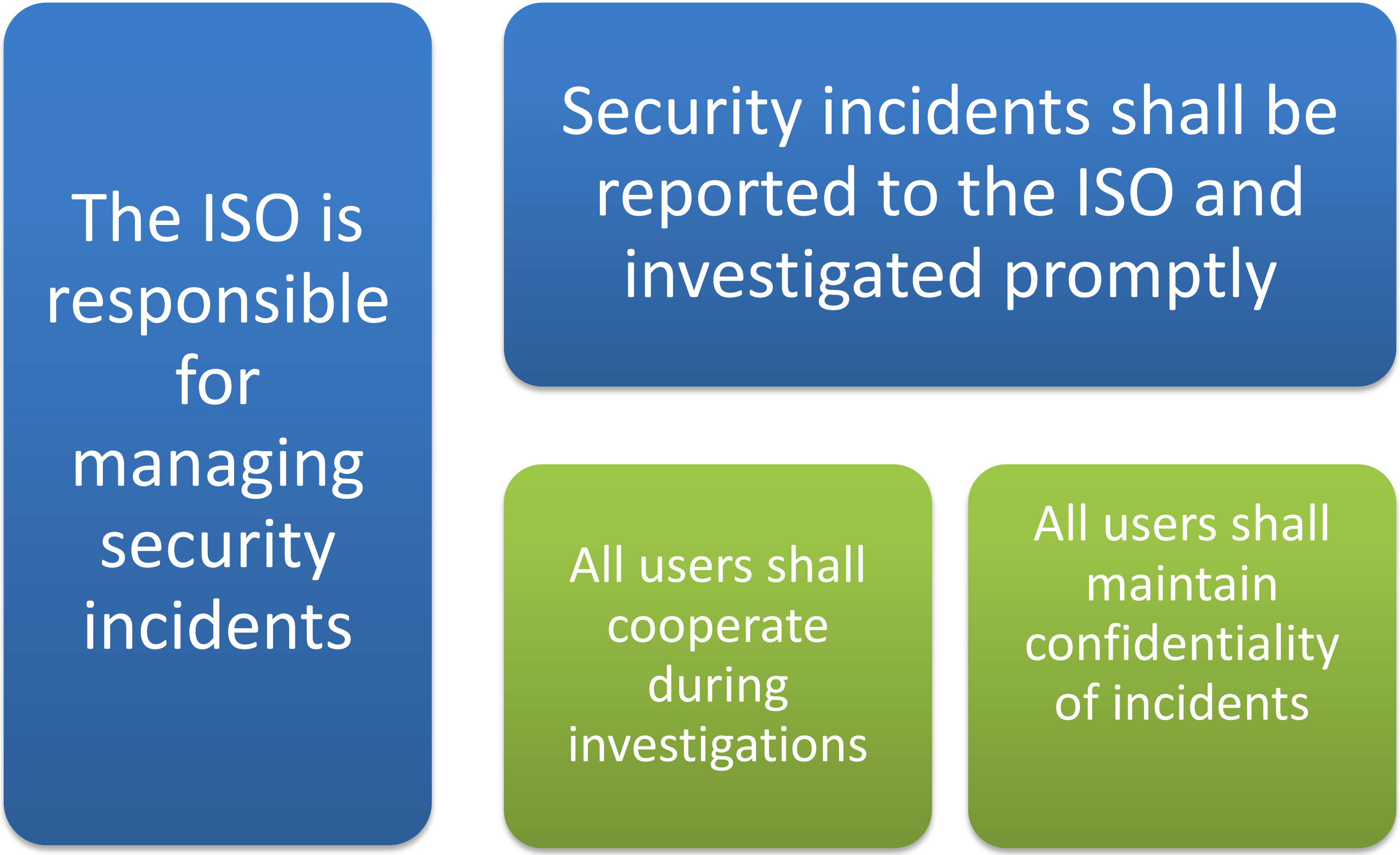
Handbook 12

Information Systems Acquisition, Development , Testing and Maintenance

- Security must be applied to all phases of the systems development lifecycle
- Must implement policies and procedures to manage operating system and software updates and patches that follow best practices
- Cryptographic Controls – Minimum requirements: confidential information transmitted over a public network, publicly accessible, or stored on a portable or personal device must be encrypted
- Vulnerability assessments may only be performed by documented, authorized individuals

4. Security Incident Management

Handbook 13



The ISO is responsible for managing security incidents

Security incidents shall be reported to the ISO and investigated promptly

All users shall cooperate during investigations

All users shall maintain confidentiality of incidents

5. Business Continuity Planning

Handbook 14

- Business continuity and disaster recovery plans must be developed for all systems and functions
- Plans must be updated as changes occur and must be reviewed at least annually
- A test of the disaster recovery plan must occur at least annually

6. Security Exceptions

Handbook 16

- Exceptions to security policy and to TAC 202 mandates must be approved by the Information Security Officer or Information Security Director
- ISO coordinates exceptions with the CIO and Information Owners

7. Sanctions

Handbook 17

- Penalties for violations of the Information Security Policy include, but are not limited to disciplinary action, loss of access and usage, termination, prosecution and/or civil action

In Summary

- Protect Confidentiality, Integrity and Availability of information and information resources by:
  - ✓ Applying the principle of least privilege
  - ✓ Using secure password practices
  - ✓ Using anti-virus and keeping it current
  - ✓ Backing up and testing data regularly
  - ✓ Documenting and following procedures
  - ✓ Maintaining and monitoring systems
  - ✓ Applying security to any device accessing our resources

http://itss.untsystem.edu/security

http://itss.untsystem.edu/it-policies

UNT | SYSTEM
IT | SHARED SERVICES
Information Security
University of North Texas System
(940) 565-7800
Paula.Mears@untsystem.edu