IT409 – IT Security and Policy

Chapter 1

Policy: “A definite course of action or procedure selected from among alternatives and in light of given conditions to guide and determine present and future decisions”.

Looking at Policy Through the Ages

The role of the Torah and Bible as written policy:

■ 3000-year old documents include business rules still in practice today.

■ First documented attempt at creating a code to preserve order.

❑ The U.S. Constitution as a Policy Revolution

■ A collection of articles and amendments that codify all aspects of American government along with citizens’ rights and responsibilities

■ A rule set with a built-in mechanism for change

❑ Both the Constitution and the Torah have a similar goal:

■ Serve as rules that guide behavior

Policy Today

■ Corporate culture

❑ Shared attitudes, values, goals, and practices that characterize a company

❑ Three classifications

■ Negative

■ Neutral

■ Positive

■ Guiding principles

❑ Reflect the corporate culture

Information Security Policy

■ A document that states how an organization plans to protect its information assets and information systems and ensure compliance with legal and regulatory requirements

❑ Asset

■ Resource with a value

❑ Information asset

■ Any information item, regardless of storage format, that represents value to the organization

■ Customer data, employee records, IT information, reputation, and brand

Successful Policy Characteristics

■ Endorsed: Management supports the policy

■ Relevant: The policy is applicable and supports the goals of the organization

■ Realistic: The policy makes sense

■ Attainable: The policy can be successfully implemented

■ Adaptable: The policy can be changed

■ Enforceable: Controls that can be used to support and enforce the policy exist

■ Inclusive: The policy scope includes all relevant parties

Defining the Role of Policy in Government

❑ Government regulation is required to protect its critical infrastructure and citizens

❑ Two major information security-related legislations were introduced in the 1990s

■ Gramm-Leach-Bliley Act (GLBA)

■ The Health Insurance Portability and Accountability Act (HIPAA)

❑ States as Leaders

■ California was the first state to enact consumer information security notification

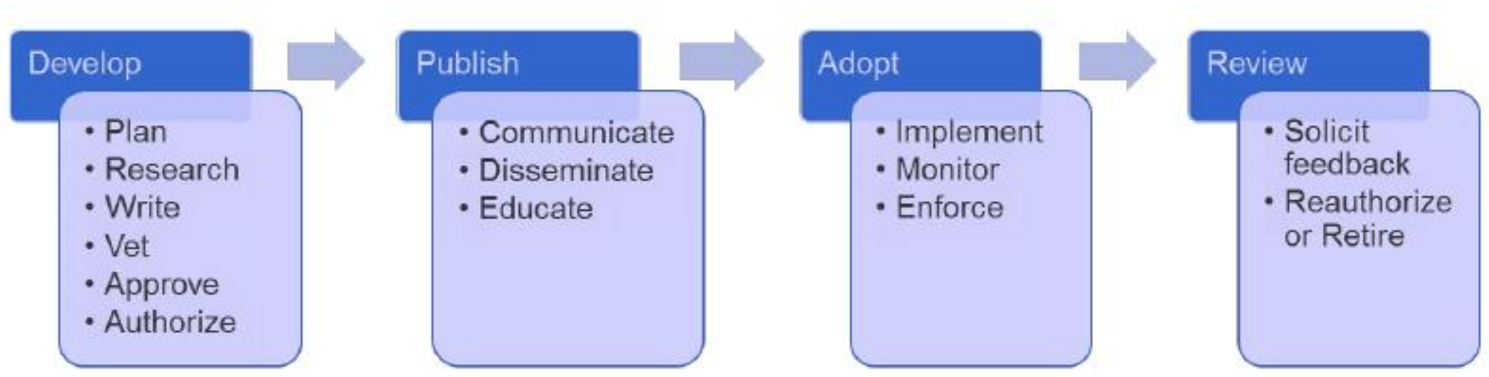
❑ SB1386: California Security Breach Information Act

❑ 46 states have passed similar legislation

■ Massachusetts was the first state to require the protection of personally identifiable information on Massachusetts residents

❑ 201 CMR 17: Standards for the Protection of Personal Information of Residents of the Commonwealth

Information Security Policy Lifecycle



Develop
- Plan
- Research
- Write
- Vet
- Approve
- Authorize

Publish
- Communicate
- Disseminate
- Educate

Adopt
- Implement
- Monitor
- Enforce

Review
- Solicit feedback
- Reauthorize or Retire

Chapter 2

Policy Hierarchy

■ Policies reflect the guiding principles and organizational objectives

■ Policies need supporting documents for context and application

❑ Standards, baselines, guidelines, and procedures support policy implementation

■ The relationship between a policy and its supporting documents is known as the policy hierarchy

■ Standards

❑ Dictate specific minimum requirements in policies

❑ They are specific

❑ Determined by management and can be changed without the Board of Director authorization

■ Note that standards change more often than policies

■ Baselines

❑ An aggregate of implementation standards and security controls for a specific category or grouping (for example, Windows 7, smartphones, and so on)

■ Guidelines

❑ Suggestions for the best way to accomplish a given task

■ Guidelines are created primarily to assist users in their goal to implement the policy

■ They are not mandatory

■ Procedures

❑ Method, or set of instructions, by which a policy is accomplished

■ A step-by-step approach to implementation

❑ Four commonly used formats for procedures

■ Simple step, hierarchical, graphic, flowchart

■ Plans and Programs

❑ Provide strategic and tactical instructions on how to execute an initiative or respond to a situation

❑ Plans and programs are used interchangeably

❑ Plans are closely related to policies

Policy Format

■ The style and format of a policy will change based on the target audience of said policy

■ Identify and understand the audience

■ Identify the culture shared by the target audience

❑ Plan the organization of the document before you start writing it. Will it be…

 ■ One document with multiple sections?

  - Consolidated policy section
- Several individual documents?
  - Singular policy

Policy Components

- Policy components
- Policies include many different sections and components
- Each component has a different purpose
- Clearly identify the purpose of each element in the planning phase before the writing part starts

Version Control

- Used to keep track of the changes to the policy
- Usually identified by a number or letter code
- Major revisions advance by a number or letter
  - 1.0, 2.0, 3.0
- Minor revisions advance by a subsection
  - 1.1, 1.2, 1.3
- Version control documentation includes:
  - Change date
  - Name of the person(s) making the change
  - Brief synopsis of the change
  - Who authorized the change
  - The effective date of the change

Introduction

- Provides context and meaning
- Explains the significance of the policy
- Explains the exemption process and the consequences of noncompliance
- Reinforces the authority of the policy
- A separate document for a singular policy
- Follows the version control table and serves as a preface for consolidated policy

Policy Headings

- Identifies the policy by name and provides an overview of the policy topic or category
- The format and content depends on the policy format
  - Singular policy includes:

        - Name of the organization or the division
        - Category, section, and subsection
        - Name of the author and effective date of the policy
        - Version number and approval authority
    - Consolidated policy document
        - Heading serves as a section introduction and includes and overview

Policy Goals and Objectives

- What is the goal of the policy?
- Introduces the employee to the policy content and conveys the intent of the policy
- One policy may have several objectives
- Singular policy objectives are located in the policy heading or in the body of the document
- Consolidated policy objectives are grouped after the policy heading

Policy Statement

- Why does the policy exist?
- What rules need to be followed?
- How will the policy be implemented?

- High- level directive or strategic roadmap
- Focuses on the specifics of how the policy will be implemented
- It’s a list of all the rules that need to be followed
- Constitutes the bulk of the policy
- Standards, procedures, and guidelines are not a part of the Policy Statement. They can, however, be referenced in that section

Policy Exceptions

- Not all rules are applicable 100% of the time
- Exceptions do not invalidate the rules, as much as they complement them by listing alternative situations
- Language used in this section must be clear, accurate, and concise so as not to create loopholes
- Keep the number of exceptions low

Policy Enforcement Clause

■ Rules and penalty for not following them should be listed in the same document

■ The level of the severity of the penalty should match the level of severity and nature of the infraction

■ Penalties should not be enforced against employees who were not trained on the policy rules they are expected to follow

Administrative Notations

■ Provides a reference to an internal resource or refers to additional information

■ Include regulatory cross-references, the name of corresponding document (standard, guideline, and so on), supporting documentation (annual reports, job descriptions), policy author name and contact information

Policy Definitions

❑ The glossary of the policy document

❑ Created and included to further enhance employee understanding of the policy and rules

❑ Renders the policy a more efficient document

❑ The target audience(s) should be defined prior to the creation of the glossary

❑ Useful to show due diligence of the company in terms of explaining the rules to the employees during potential litigation

Writing Style and Technique

■ Sets the first impression

■ Policies should be written using plain language

  ❑ Simplest, most straightforward way to express an idea

  ❑ Follow The Plan Language Action and Information Network (PLAIN) guidelines

Chapter 3

CIA

The CIA Triad or CIA security model

- Stands for Confidentiality, Integrity, and Availability
- An attack against either or several of the elements of the CIA triad is an attack against the Information Security of the organization
- Protecting the CIA triad means protecting the assets of the company

What Is Confidentiality?

- Not all data owned by the company should be made available to the public
- Failing to protect data confidentiality can be disastrous for an organization:
    - Dissemination of Protected Health Information (PHI) between doctor and patient
    - Dissemination of Protected Financial Information (PFI) between bank and customer
    - Dissemination of business-critical information to rival company
- Only *authorized users* should gain access to information
- Information must be protected when it is used, shared, transmitted, and stored
- Information must be protected from unauthorized users both internally and externally
- Information must be protected whether it is in digital or paper format
- The threats to confidentiality must be identified. They include:
    - Hackers and hacktivists
    - Shoulder surfing
    - Lack of shredding of paper documents
    - Malicious Code (Virus, worms, Trojans)
    - Unauthorized employee activity
    - Improper access control

What Is Integrity?

- Protecting data, processes, or systems from intentional or accidental unauthorized modification
    - Data integrity
    - System integrity
- A business that cannot trust the integrity of its data is a business that cannot operate

- An attack against data integrity can mean the end of an organization's capability to conduct business
- Threats to data integrity include:
    - Human error
    - Hackers
    - Unauthorized user activity
    - Improper access control
    - Malicious code
    - Interception and alteration of data during transmission
- Controls that can be deployed to protect data integrity include:
    - Access controls:
        - Encryption
        - Digital signatures
    - Process controls
        - Code testing
    - Monitoring controls
        - File integrity monitoring
        - Log analysis
    - Behavioral controls:
        - Separation of duties
        - Rotation of duties
        - End user security training

What Is Availability?

Availability: The assurance that the data and systems are accessible when needed by authorized users

- What is the cost of the loss of data availability to the organization?

- A risk assessment should be conducted to more efficiently protect data availability
- Threats to data availability include:
    - Natural disaster
    - Hardware failures
    - Programming errors
    - Human errors
    - Distributed Denial of Service attacks
    - Loss of power
    - Malicious code

- Temporary or permanent loss of key personnel

The Five A's of Information Security

- Accountability
    - All actions should be traceable to the person who committed them
    - Logs should be kept, archived, and secured
    - Intrusion detection systems should be deployed
    - Computer forensic techniques can be used retroactively
    - Accountability should be focused on both internal and external actions
- Assurance
    - Security measures need to be designed and tested to ascertain that they are efficient and appropriate
    - The knowledge that these measures are indeed efficient is known as assurance
    - The activities related to assurance include:
        - Auditing and monitoring
        - Testing
        - Reporting
- Authentication
    - Authentication is the cornerstone of most network security models
    - It is the positive identification of the person or system seeking access to secured information and/or system
    - Examples of authentication models:
        - User ID and password combination
        - Tokens
        - Biometric devices
- Authorization
    - Act of granting users or systems actual access to information resources
    - Note that the level of access may change based on the user's defined access level
    - Examples of access level include the following:
        - Read only

        - Read and write
        - Full

- Accounting
    - Defined as the logging of access and usage of resources
    - Keeps track of who accesses what resource, when, and for how long
    - An example of use:
        - Internet café, where users are charged by the minute of use of the service

Who Is Responsible for CIA?

- Information owner
    - An official with statutory or operational authority for specified information
    - Has the responsibility for ensuring information is protected from creation through destruction
- Information custodian
    - Maintain the systems that store, process, and transmit the information

Information Security Framework

- Two of the most widely used frameworks are:
    - Information Technology and Security Framework by NIST
    - Information Security Management System by ISO

NIST Functions

- Founded in 1901
- Nonregulatory federal agency
- Its mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve quality of life
- Published more than 300 information security-related documents including
    - Federal Information Processing Standards

  - Special Publication 800 series
  - ITL bulletins

ISO Functions

- A network of national standards institutes of 146 countries
- Nongovernmental organization that has developed more than 13,000 international standards
- The ISO/IEC 27000 series represents information security standards published by ISO and Electro-technical Commission (IEC)

ISO 27002:2013 Code of Practice

- Comprehensive set of information security recommendations on best practices in information security
- ISO 27002:2013 is organized in the following domains:
  - Information security policies (Section 5)
  - Organization of information security (Section 6)
  - Human Resources security (Section 7)
  - Asset management (Section 8)
  - Access control (Section 9)
  - Cryptography (Section 10)
  - Physical and environmental security (Section 11)
  - Operations security (Section 12)
  - Communications security (Section 13)
  - Information systems acquisition, development, and maintenance (Section 14)
  - Supplier relationships (Section 15)
  - Information security incident management (Section 16)
  - Business continuity (Section 17)
  - Compliance management (Section 18)

Chapter 4

Understanding Information Security Policies

- The goal of the information security policies is to protect the organization from harm
  - Policies should be written
  - Policies should be supported by management
  - Policies should help companies align security with business requirements and relevant laws and regulations
- ISO 27002:2013 can provide a framework for developing security policies
- Two approaches to information security
  - Parallel approach
  - Integrated approach
- Policies can serve as teaching documents to influence behavior
  - Acceptable Use Policy
- Companies should create vendor versions of information security policies
- Policies should be authorized by executive management
- Policies should be updated on regular basis

Evaluating Information Security Policies

- Policies can be evaluated internally or by independent third parties
- Audit
  - Systematic, evidence-based evaluation
  - Include interviews, observation, tracing documents to management policies, review or practices, review of documents, and tracing data to source documents
  - Audit report containing the formal opinion and findings of the audit team is generated at the end of the audit
- Capability Maturity Model (CMM)
  - Used to evaluate and document process maturity for a given area

Information Security Governance

- The process of managing, directing, controlling, and influencing organizational decisions, actions, and behaviors
- The Board of Directors is usually responsible for overseeing the policy development
- Effective security requires a distributed governance model with the active involvement of stakeholders, decision makers, and users

Distributed Governance Model

- Chief information security officer (CISO)
- Information security steering committee
- Compliance officer
- Privacy officer
- Internal audit
- Incident response team
- Data owners
- Data custodians
- Data users

Regulatory Requirements

- Gramm-Leach Bliley (GLBA) Section 314.4
- HIPAA/HITECH Security Rule Section 164.308(a)
- Payment Card Industry Data Security Standard (PCI DDS) section 12.5
- 201 CMR 17: Standards for Protection of Personal Information of the Residents of the Commonwealth–Section 17.0.2

Information Security Risk

- Three factors influence information security decision making and policy creation
  - Guiding principles
  - Regulatory requirements
  - Risk associated with achieving business objectives
- Risk: The potential of undesirable or unfavorable outcome from a given action
- Risk tolerance: how much undesirable outcome the risk taker is willing to accept
- Risk appetite: The amount of risk an entity is willing to accept in pursuit of its mission

Risk Assessment

- Evaluate what can go wrong and the likelihood of a harmful event occurring
- Risk assessment involves
  - Identifying the inherent risk based on relevant threats, threat sources, and related vulnerabilities
  - Determining the impact of a threat if it occurs
  - Calculating the likelihood of occurrence
  - Determining residual risk
- Inherent risk
  - The level of risk before security measure are applied

- Residual risk
  - The level of risk after security measures are applied
- Threat
  - Natural, environmental, or human event that could cause harm
- Vulnerability
  - A weakness that could be exploited by a threat
- Impact
  - The magnitude of a harm

Risk Assessment Methodologies

- Components of a risk assessment methodology include
  - Defined process
  - Assessment approach
  - Standardized analysis
- Three well-known information security risk assessment methodologies
  - Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
  - Factor Analysis of Information Risk (FAIR)
  - NIST Risk Management Framework (RMF)

Risk Management

- The process of determining an acceptable level of risk, calculating the current risk level, accepting the level of risk, or taking steps to reduce it to an acceptable level
  - Risk acceptance
  - Risk mitigation
- Risk reduction
- Risk transfer
- Risk sharing
- Risk avoidance

Chapter 5

Information Assets and Systems

■ What is an information asset?

❑ A definable piece of information, stored in any manner, and recognized as having value to the organization

❑ The information is used by the company (regardless of size) to fulfill its mission or goal

❑ Could be any information, such as customer and employees data, research and proprietary data, intellectual property data, and operational plans and procedures that have value to the company

■ Information Systems

❑ Provide a way and a place to process, store, transmit, and communicate the information

❑ Usually a combination of both hardware and software assets

❑ Can be off-the-shelf or customized systems

■ Information Ownership

❑ ISO stands for information security officer

❑ The ISO is accountable for the protection of the organization. Compare this with:

■ The information owner is responsible for the information he owns

■ The information custodian is responsible for implementing the actual controls that protect the information assets

❑ The ISO is the central repository of security information

Information Classification

■ Definitions:

❑ Information Classification

■ Information classification is the organization of information assets according to their sensitivity to disclosure

❑ Classification Systems

■ Classification systems are labels that we assign to identify the sensitivity levels

■ Federal Information Processing Standard 199 (FIPS-199) requires information owners to classify information and information systems based on CIA criteria as:

❑ Low potential impact

❑ Moderate potential impact

❑ High potential impact

■ Government & Military Classification Systems

❑ Top Secret (TS)

❑ Secret (S)

❑ Confidential (C)

❑ Unclassified (U)

❑ Sensitive But Unclassified (SBU)

❑ Top Secret (TS)

■ Applied to "any information or material the unauthorized disclosure of which reasonably could be expected to cause an exceptionally grave damage to the national security"

❑ Secret (S)

■ Applied to "any information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security"

❑ Confidential (C)

■ Applied to "any information or material the unauthorized disclosure of which reasonably could be expected to cause damage to the national security"

❑ Unclassified (U)

■ Applied to "any information that can generally be distributed to the public without any threat to national interest"

❑ Sensitive But Unclassified (SBU)

■ Applied to "any information of which the loss, misuse or unauthorized access to, or modification of might adversely affect U.S. National Interests, the conduct of the Department of Defense (DoD) programs or the privacy of DoD personnel"

■ Commercial classification systems:

❑ No standard: Each company can choose its own system that matches its culture and needs

❑ Usually less complex than the government system

❑ The more regulated a company, the more complex the classification system it adopts

■ Commercial classification systems

❑ Most systems revolve around these four classification levels:

❑ Protected

❑ Confidential

❑ Internal Use

❑ Public

■ Commercial classification systems

❑ Protected

■ Data protected by law, regulation, memorandum of agreement, contractual obligation, or management discretion

■ Examples: Social Security numbers, personal health information, financial information

❑ Confidential

■ Data essential to the mission of an organization

■ Only available to a small circle of authorized individuals

■ Disclosure would cause significant financial loss, reputation loss and/or legal liability

■ Commercial classification systems

❑ Internal Use:

■ Data necessary for conducting ordinary company business

■ Loss, disclosure, and corruption may impair the business and lead to business, financial, or legal loss

❑ Public:

■ Information that does not require protection

■ Information that is specifically intended for the public

Reclassification/Declassification

❑ The need to protect information may change

❑ With that change, the label assigned to that information may change as well

❑ The process of downgrading sensitivity levels is called declassification

❑ The process of upgrading sensitivity levels is called reclassification

Labeling and Handling Standards

■ Information labeling:

❑ Labeling is the vehicle for communicating the assigned classification to information custodians and users

❑ Labels must be clear and self-explanatory

❑ In electronic form, the label should be made part of the filename

❑ In printed form, the label should be clearly visible on the outside and in the header and/or footer

■ Information handling:

❑ Information must be handled in accordance with its classification

❑ The information user is responsible for using the information in accordance with its classification level

Labeling and Handling Standards

■ Information labeling:

❑ Labeling is the vehicle for communicating the assigned classification to information custodians and users

❑ Labels must be clear and self-explanatory

❑ In electronic form, the label should be made part of the filename

❑ In printed form, the label should be clearly visible on the outside and in the header and/or footer

■ Information handling:

❑ Information must be handled in accordance with its classification

❑ The information user is responsible for using the information in accordance with its classification level

Information Systems Inventory

■ Many organizations don't have an up-to-date inventory

■ Creating a comprehensive inventory of information systems is a major task

■ Both hardware and software assets should be inventoried

■ Each asset should have a unique identifier and a description

■ Company assets should be accounted for at all times

■ An asset management procedure should exist for moving and destroying assets

❑ Hardware assets include (but are not limited to):

■ Computer equipment

■ Printers

■ Communication and network equipment

■ Storage media

■ Infrastructure equipment

❑ Software assets include (but are not limited to):

■ Operating system software

■ Productivity software

■ Application software

Chapter 6

The Employee Lifecycle

■ Represents stages in the employee’s career

■ Lifecycle models can vary but most include the following stages

❑ Recruitment

❑ Onboarding

❑ User provisioning

❑ Orientation

❑ Career development

❑ Termination

What Does Recruitment Have to Do with Security?

❑ Risks and rewards of posting online employment ads:

■ A company can reach a wider audience

■ A company can publish an ad that gives too much information:

❑ About the network infrastructure and therefore allow a hacker to footprint the internal network easily and stealthily

❑ About the company itself, inviting social engineering attacks

Job Postings

■ Job descriptions are supposed to:

❑ Convey the mission of the organization

❑ Describe the position in general terms

❑ Outline the responsibilities attached to said position

❑ Outline the company’s commitment to security via the use of such terms as non-disclosure agreement

■ Job descriptions are NOT supposed to:

❑ Include information about specific systems, software versions, security configurations, or access controls

■ It’s harder to hack a network if one doesn’t know what hardware & software

❑ If the above information is deemed necessary, two versions of the position can be created. The second, more detailed version should be posted internally and shared with candidates that have made the “first cut”

Candidate Application Data

■ Companies are responsible for protecting the data and privacy of the job seeker

■ Non-public personal information (NPPI) should not be collected if possible

The Interview

■ Job Interview:

❑ The interviewer should be concerned about revealing too much about the company during the interview

❑ Job candidates should never gain access to secured areas

❑ A job interview is a perfect foot-printing opportunity for hackers and social engineers

Screening Prospective Employees

❑ An organization should protect itself by running extensive background checks on potential employees at all levels of the hierarchy

❑ Some higher level positions may require even more in-depth checks

❑ Many U.S. government jobs require prospective employees have the requisite clearance level

Types of Background Checks

❑ The company should have a basic background check level to which all employees are subjected

❑ Information owners may require more in-depth checks for specific roles

❑ Workers also have a right to privacy: Not all information is fair game to gather – only information relevant to the actual work they perform

❑ Companies should seek consent from employees before launching a background check

❑ Educational records fall under FERPA. Schools must first have written authorization before they can provide student-related information

❑ Motor vehicle records fall under DPPA, which means that the DMV – or its employees – are not allowed to disclose information obtained by the department

❑ The FTC allows the use of credit reports prior to hiring employees as long as companies do so in accordance with the Fair Credit Reporting Act

❑ Bankruptcies may not be used as the SOLE reason to not hire someone according to Title 11 of the U.S. Bankruptcy Code

❑ Criminal history: The use of this sort of information varies from state to state

❑ Worker’s compensation records: In most states, these records are public records, but their use may not violate the Americans with Disabilities Act

What Happens in the Onboarding Phase?

■ The new hire is added to the organization’s payroll and benefit systems

■ New employees must provide

❑ Proof of identity

❑ Work authorization

❑ Tax identification

■ Two forms that must be completed

❑ Form I-9

❑ Form W-4

What Is User Provisioning?

■ The process of:

❑ Creating user accounts and group memberships

❑ Providing company identification

❑ Assigning access rights and permissions

❑ Assigning access devices such as tokens and/or smartcards

■ The user should be provided with and acknowledge the terms and conditions of the Acceptable Use Agreement before being granted access

What Should an Employee Learn During Orientation?

■ His responsibilities

■ Information handling standards and privacy protocols

■ Ask questions

The Importance of Employee Agreements

❑ Confidentiality or non-disclosure agreements

■ Agreement between employees and organization

■ Defines what information may not be disclosed by employees

■ Goal: To protect sensitive information

■ Especially important in these situations:

❑ When an employee is terminated or leaves

❑ When a third-party contractor was employed

■ Acceptable Use Agreement

❑ A policy contract between the company and information systems user

■ Components of an Acceptable Use Agreement

❑ Introduction

❑ Data classifications

❑ Applicable policy statement

❑ Handling standards

❑ Contacts

❑ Sanctions for violations

❑ acknowledgment

The Importance of Security Education and Training

■ Training employees

❑ According to NIST: "Federal agencies […] cannot protect […] information […] without ensuring that all people involved […]:

■ Understand their role and responsibilities related to the organization's mission

■ Understand the organization's IT security policy, procedures and practices

■ Have at least adequate knowledge of the various management, operational and technical controls required and available to protect the IT resources for which they are responsible"

■ Hackers adapt: If it is easier to use social engineering – i.e., targeting users – rather than hack a network device, that is the road they will take

■ Only securing network devices and neglecting to train users on information security topics is ignoring half of the threats against the company

What Is the SETA Model?

■ What is SETA?

❑ Security Education Training and Awareness

❑ Awareness is not training: It is focusing the attention of employees on security topics to change their behavior

❑ Security awareness campaigns should be scheduled regularly

❑ Security training "seeks to teach skills" (per NIST)

❑ Security training should NOT be dispensed only to the technical staff but to all employees