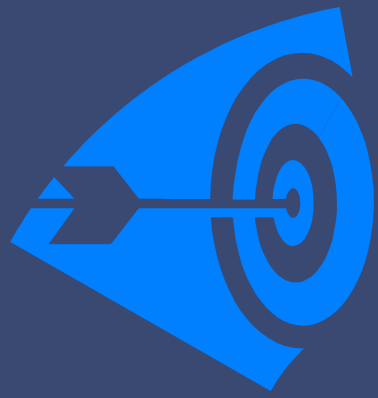
Course: Information Security Management in e-Governance

Day 2

Session 4: Information Security Policy and Organization

Agenda



- Need for Information Systems Security Policy
- Elements of Information Security Policy
- Approach for development of Information Security Policy
- Information Security Organization and roles, responsibilities

Security Policy

One of the desired features of an **electronic government** is to guarantee that:

- confidential data held in the system is fully protected.
- network be protected from unauthorized access, malicious attack and loss of data integrity

- Poor security can leads to inability to function and lose of data, incur more cost to fix and recover data, disruption to government operation, and damage reputation.

- Security policy needs to be defined to protect the **government assets** as well as to provide better and faster response to security incidents.

Security Policy contd..

The assets that must be protected include:

- Computer and Peripheral Equipment.
- Communications Equipment.
- Computing and Communications Premises.
- Power, Water, Environmental Control, and Communications utilities.
- Supplies and Data Storage Media.
- System Computer Programs and Documentation.
- Application Computer Programs and Documentation.
- Information.

A well defined Security Policy will help government organizations

- To minimize the adverse effect of security incidents
- To educate users of information assets security measures
- To provide a mechanism for reporting of security incidents so that remedy / action can be taken quickly
- To ensure that security measures/guidelines are adhered to by users
- To formulate and review policies, goals, strategies, standard and operational guidelines pertaining to information security of the Central / state government

A well defined Security Policy will help government organizations contd..

- To monitor, review and co-ordinate the implementation of central / state security measures among state public agencies
- To establish standard in the application security measures
- To carry out auditing on central / state assets so that security measures/guidelines are adhered to
- To take pre-emptive actions to remove possible source of vulnerabilities

Information security policies

- ***Information security policies*** are a special type of documented business rule for protecting information and the systems which store and process the information.
- Within an organization, these written policy documents provide a high-level description of the various controls the organization will use to protect information.
- It is a formal declaration of management's intent to protect information, and are required for compliance with various security and privacy regulations.
- Lays down the rules through which people are given access to an organization’s technology, system and information assets.

Information security policies contd..

- Security policies define the overall security and risk control objectives that an organization endorses
- Set of detailed rules as to what is allowed on the system and what is not allowed.
- The security policy defines what business and security goals and objectives management desires, but not how these solutions are engineered and implemented.

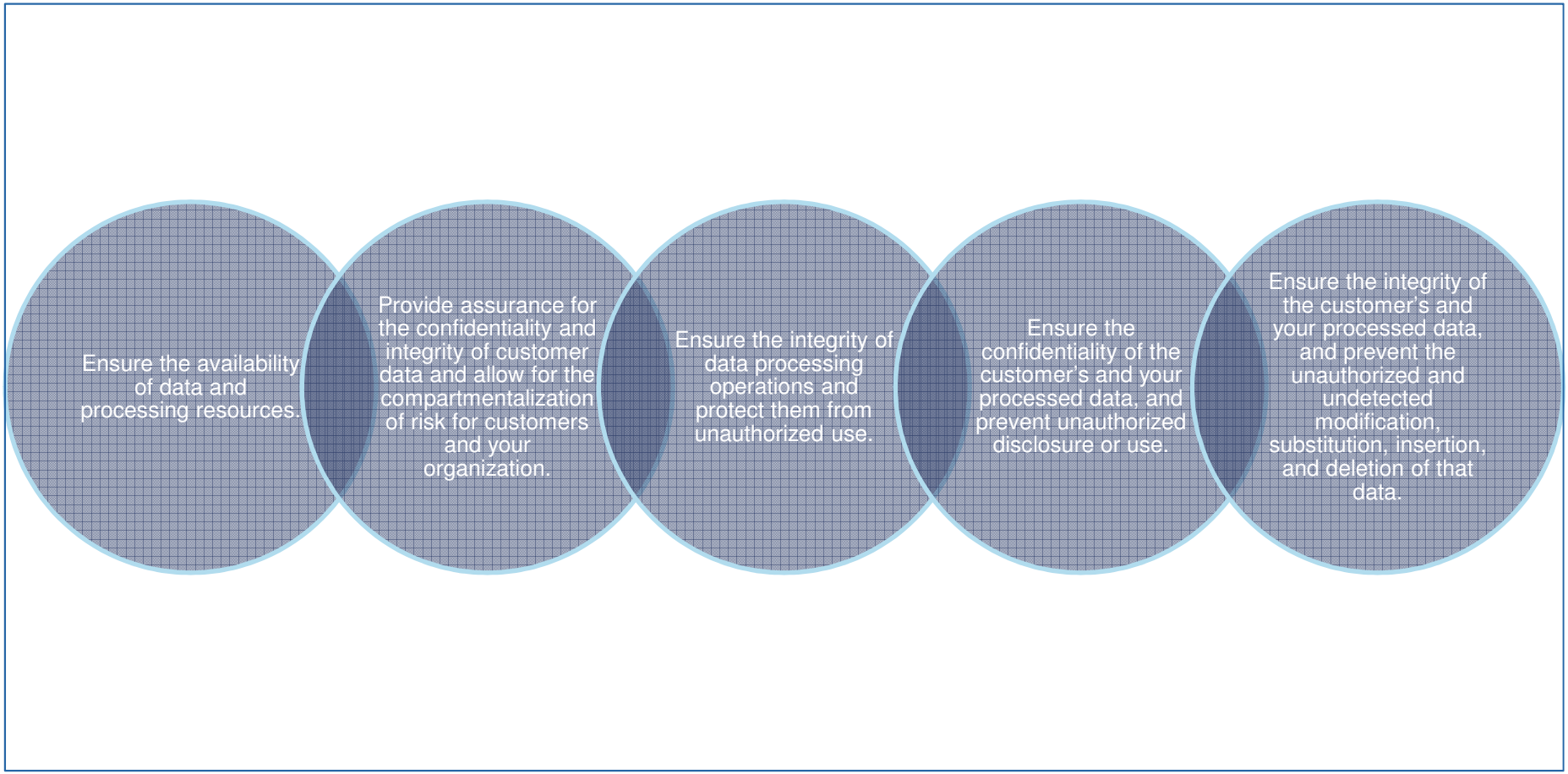
Purposes of a Security Policy

- The primary purpose of a security policy is to inform users, staff, and managers of those essential requirements for protecting various assets including people, hardware, and software resources, and data assets.
- Using, managing and distributing such information – in any form, electronic or physical - in a manner that is consistent with those requirements.
- Provide a baseline from which to acquire, configure, and audit computer systems and networks for compliance with the policy.
- Subsequent development of operational procedures, the establishment of access control rules and various application, system, network, and physical controls and parameters.

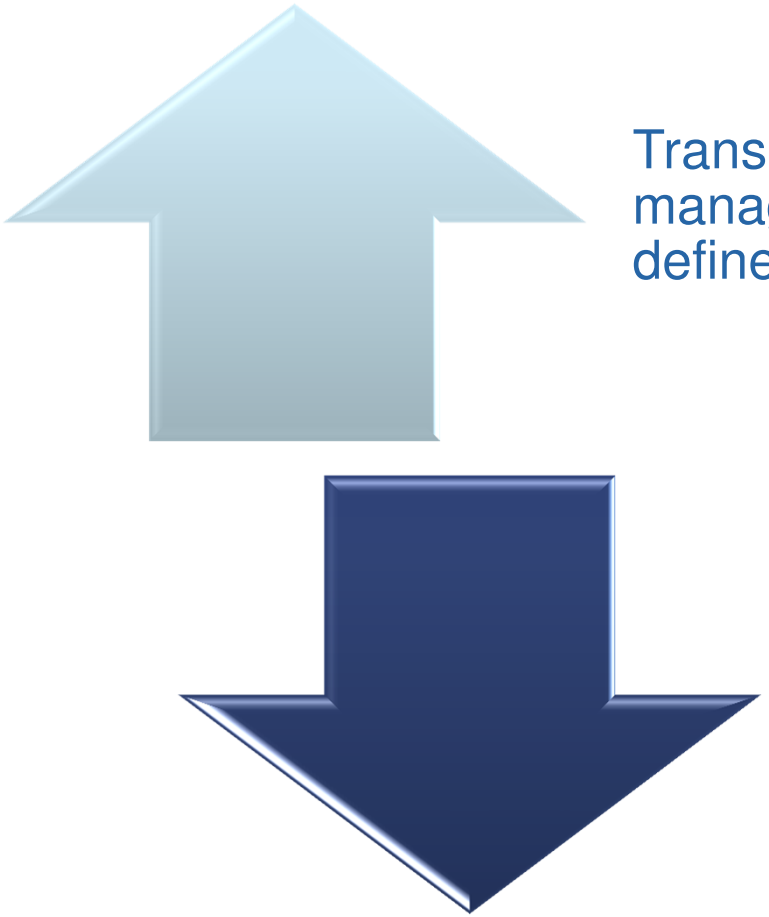
Security Principles

- The definition of security principles is an important first step in **security policy development** as they dictate the specific type and nature of security policies most applicable to one's environment.
- Security principles are used to define a foundation upon which security policies can be further defined.
- Organizations should evaluate and review these security principles before and after the development and elaboration of security policies.

The principles for security policies are based upon the following goals:



Security Policy Goals



Translate, clarify and communicate management's position on security as defined in high-level security principles.

The security policies act as a bridge between these management objectives and specific security requirements.

The policy deals with the following domains of security

- Computer system / Network security: CPU, Peripherals, OS. This includes data security.
- Physical security: The premises occupied by the IT personnel and equipment.
- Operational security: Environment control, power equipment, operation activities.
- Procedural security by IT, vendor, management personnel, **as well as ordinary users**.
- Communications security: Communications equipment, personnel, transmission paths, and adjacent areas.

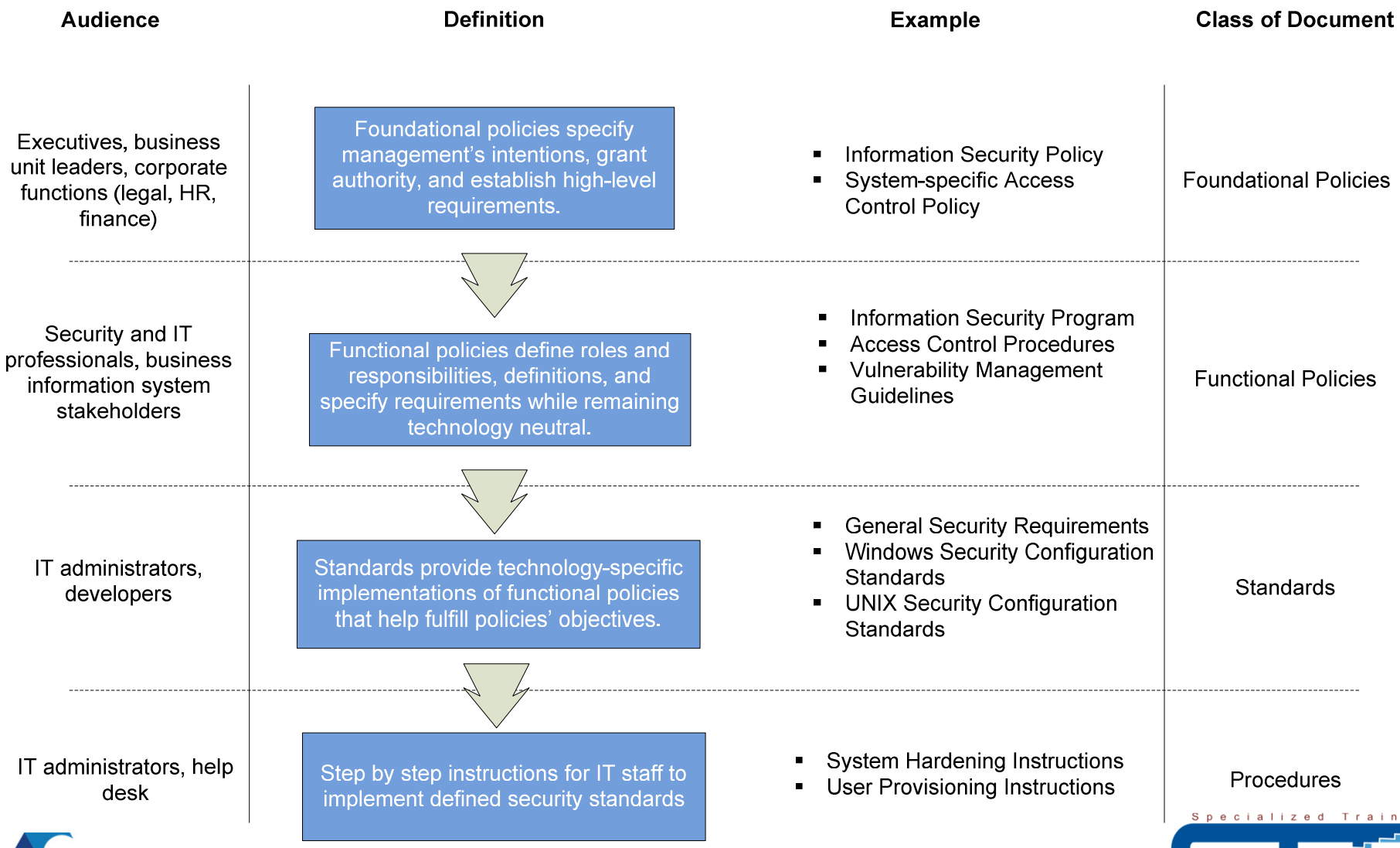
Types of information security policy documents

- Acceptable Use Policy
- Authentication Policy
- Backup Policy
- Confidential Data Policy
- Data Classification Policy
- Encryption
- Email Policy
- Policy
- Guest Access Policy
- Incident Response Policy
- Mobile Device Policy
- Network Access Policy
- Network Security policy
- Outsourcing Policy
- Password Policy
- Physical Security policy
- Remote Access Policy
- Retention Policy
- Third Party Connection Policy
- VPN Policy
- Wireless Access Policy
- Many others

Elements of an information security policy document

- An ideal information security policy document should contain the following elements:
  - Title - Brief description of the document.
  - Number - A number or unique identifier for the policy document.
  - Author - The author of the document.
  - Publish Date - The date the policy has been officially approved.
  - Scope - Describes the organizational scope that this policy applies to.
  - Policy Text - The written policies.
  - Sanctions - Provides information on violations of the written policy.
  - Sponsor - The executive sponsor of the policy document.

Policy Hierarchy



Characteristics of good security policies

- They must be **implementable through system administration procedures,** publishing of acceptable use guidelines, or other appropriate methods.
- They must be **enforceable with security tools, where appropriate, and with** sanctions, where actual prevention is not technically feasible.
- They must clearly define the areas of **responsibility for the users, administrators,** and management.
- They must be **documented, distributed, and communicated.**

Policy Flexibility

- A successful security policy must be flexible.
- In order for a security policy to be viable for the long term, a security policy should be independent of specific hardware and software decisions, as specific systems choices change rapidly.
- In addition, the mechanisms for updating the policy should be clearly spelled out.
- This includes the process, the people involved, and the people who must sign-off on the changes.

Security Policy Communication

- Disseminate Policy to all appropriate users, staff, management, vendors, third party processors, and support personnel.
- May also be necessary to communicate some or all policies to customers / citizens as well.
- Establishing a record that those involved have read, understood, and agreed to abide by the policy is an essential part of this process.

Policy Management

- To ensure that your policies do not become obsolete, you should implement a regular review process of them.
- That process should include some form of update mechanism so that changes in your organization's operating environment can be quickly translated into your security policy.

Relationship to Standards and Procedures

- Security policies embody management's overall security expectations, goals and objectives.
- To be practical and implementable, policies must be further defined by standards, guidelines, and procedures.
- These must ensure that all operations are consistent with the intent of the security policies.

Relationship to Standards and Procedures

- Standards, guidelines, and procedures provide specific interpretation of policies and instruct users, customers, technicians, management, and others on how to implement the policies.
- Organization should undertake the definition of standards, guidelines, and procedures only after the development and acceptance of security policies, and after specific security mechanisms supporting these policies are determined or implemented.

Security Policy Structure

The basic structure of a security policy should contain the following components:

- A statement of the issue that policy addresses.
- A statement about your position on the policy.
- How the policy applies in the environment.
- The roles and responsibilities of those affected by the policy.
- What level of compliance to the policy is necessary.
- What actions, activities and processes are allowed and which are not.
- What are the consequences of non-compliance.

Roles and Responsibilities

The development of security policies is predicated upon the participation of various organizations.

In general, it is recommended that the following areas participate in this development effort:

- Business management
- Technical management
- Data security
- Risk management
- Systems operations
- Application development
- Network engineering
- Systems administration
- Internal audit
- Legal
- Human resources

Recommended Development Method

The following provides an outline of the tasks used to develop security policies

- All responsible organizations and stakeholders are identified and their roles, obligations and tasks detailed.
  - It is important to understand how your organization is structured, who will be the responsible owner of the security policy and also who will function as its custodian.
  - Critical to obtain the appropriate level of consensus to ensure that the security policy properly reflects the issues, concerns, requirements, goals, and objectives for your organization.
  - Representation should be as broad as practical but at a minimum include: data security, legal, human resources, internal audit, operations, and development organizations.

Recommended Development Method (contd..)

- The primary business objectives are outlined.
  - Knowing the primary objectives of your business is important to scoping the security policy effort.
  - For example, one organization may require extensive audit, monitoring, and backup and recovery processes because of regulatory mandates while this may not be applicable to another.
  - The intent here is to make security policy cost effective.
  - That is, do what is appropriate for your organization, not the security consultant selling you the security policies!!

Recommended Development Method (contd..)

A list of security principles representing management's security goals is outlined.

- Accompanying this article is a list of security principles.
- These should be reviewed and incorporated into your security policy development effort as necessary.
- The purpose of the security principles is to allow your organization to state in a plain and simple fashion, without technical details or jargon, what core values are most important to your organization.

Recommended Development Method (contd..)

All applicable data and processing resources are identified and classified.

- In today's IT environments, data is often one of the most important assets and should be treated accordingly.
- For that reason, cataloging your data and processing resources enables you to more easily make qualified and informed decisions about their use and value.
- This then enables you to later apply the most cost effective controls on those assets.

Recommended Development Method (contd..)

A data flow analysis is performed for the primary data classifications, from generation through deletion.

- The purpose of a data flow analysis is to allow you to identify all of the trust points that touch your data.
- For instance, in a transaction processing system, data may flow through browsers, web, data, and other servers or firewalls and be stored in databases, on magnetic tape or paper.
- By tracing the flow of your data assets through your processing assets, you can later determine the type and placement of logical and physical controls to protect those assets.

Recommended Development Method (contd..)

The primary threats that can reasonably be expected in one's environment are outlined.

- The development of a threat profile enables you to decide what type of threats exist in your particular environment, what the probability is of a threat manifesting itself into an actual problem, and what the ramifications, costs and consequences are of those threats being realized.

- Remember, threats vary widely between different environments.

- The threats and consequences of attacks to a financial network processing monetary instruments will be different than the threats and consequences of attacks to an online government application.

Recommended Development Method (contd..)

The primary security services necessary in the environment are identified.

- After your data and processing assets are identified and a threat profile created, the next step is to determine what general security services would be appropriate in your environment.
- These security services are high-level and can include for example: accountability, authorization, availability, identification, authentication, confidentiality, integrity, and non-repudiation.
- Knowing what security services your environment requires will drive the selection of the types of security policies you will need as well as the specific content or components of those policies.

Recommended Development Method (contd..)

A generic policy template is constructed.

- The structure of a security policy can take many forms.
- This article offers recommendations for both the components and characteristics of security policies.
- This step is used to articulate the specific topics that you consider necessary for each security policy.

Recommended Development Method (contd..)

A list of security policies is defined.

- The last step before actually drafting the security policies themselves is to identify all of the security policy focus areas that must be addressed.
- The creating of this list is based upon the results of the above steps.

Security Policy Implementation

Once you've created your policy, you need to roll it out to your organization.

- First, and perhaps most importantly, a security policy must be backed by your Organization's senior management team.
- If the position doesn't exist, an Information Security Officer should be designated who is responsible for implementing and managing the security policy.
- Go through each policy and think about how it will be applied within the organization.
- Make sure that the tools are in place to conform to the policy.

Security Policy Implementation contd..

- For example, if the policy specifies that a certain network be monitored, make sure that monitoring capabilities exist on that network segment.
- If a policy specifies that visitors must agree to the Acceptable Use Policy before using the network, make sure that there is a process in place to provide visitors with the Acceptable Use Policy.

Security Policy Implementation contd..

- User education is critical to a successful security policy implementation.
- A training session should be held to go over the specific policies that will impact users, as well as provide basic information security awareness training.
- Users must be provided any user-level policies, and must acknowledge in writing that they have read and will adhere to the policies.

Security Policy Implementation contd..

- No matter how well thought out, no policy will be 100% applicable for every scenario, and exceptions will need to be granted.
- Exceptions, however, must be granted only in writing and must be well documented.
- It should be made clear from the outset that the policy is the official standard, and an exception will only be granted when there is an overwhelming business need to do so.

Policy Review

- After the security policy has been in place for some period of time, the Organization's information security controls should be audited against the applicable policies.
- Make sure that each policy is both A) being followed, and B) still appropriate to the situation.
- Regularly review the security policy to ensure that it still meets Organization's requirements.
- Create a process so that the policy is periodically reviewed by the appropriate persons.

Policy Review contd..

- Review should occur both at certain intervals (i.e., once per year), and when certain business changes occur (i.e., the company opens a new location).
- This will ensure that the policy does not get “stale” and will continue to be a useful management tool for years to come

End of Session