Cyber Security
Unit - II

Dr. R. A. ROSELINE M.Sc., M.Phil., Ph.D.,
Associate Professor and Head,
Post Graduate Department Of Computer Applications,
Government Arts College, Coimbatore – 18.

Contents

- **Information security policy**
  - Policy is the Cornerstone
  - Why Implement an Information Security Policy
  - Corporate Policies
  - Organization wide (Tier1) Policies
  - Organization wide Policy Document
  - Legal Requirements
  - Business Requirements
  - Definitions
  - Policy Key Elements
  - Policy Format

Information Security Policies

Policy Is the Cornerstone

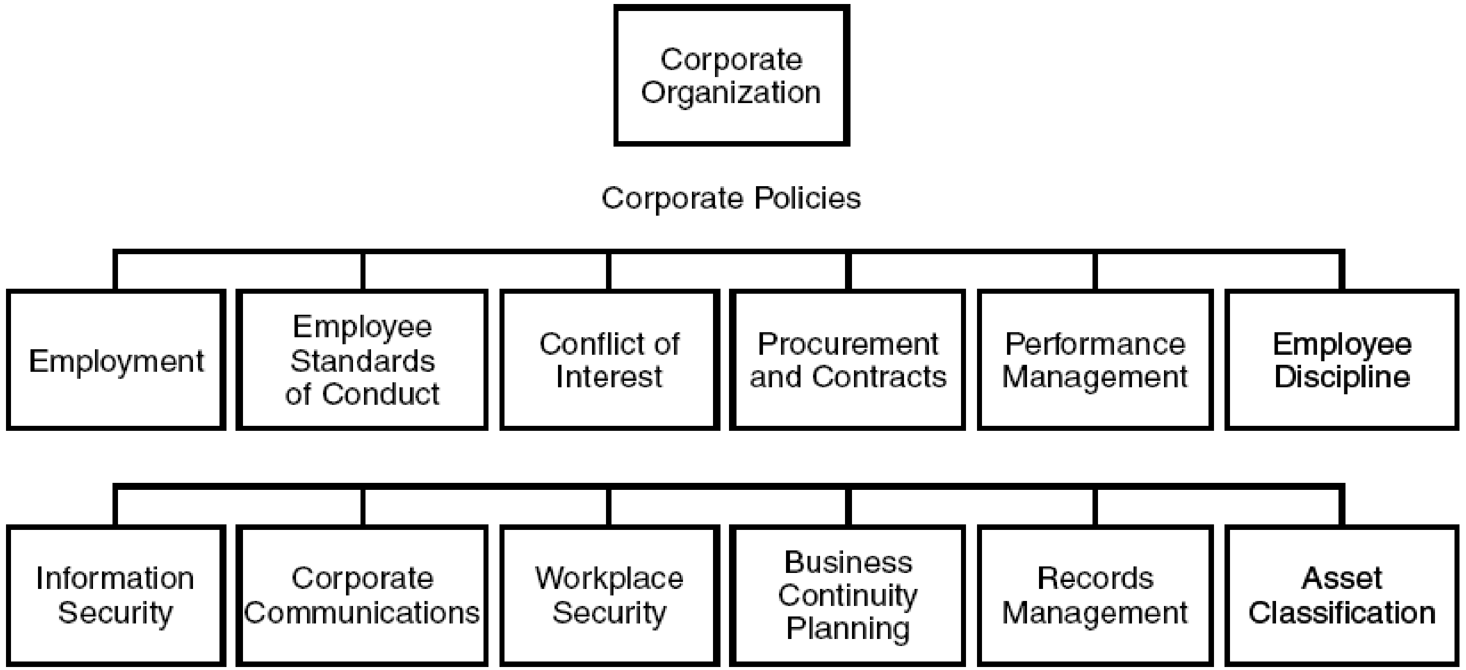
1. The cornerstone of effective information security architecture is a well written policy statement. This is the wellspring of all other directives, standards, procedures, guidelines, and other supporting documents.
2. As with any foundation, it is important to establish a strong footing. As will be discussed, a policy performs two roles: one internal and one external.

Why Implement an Information Security Policy

The policies initially discussed are high-level organization wide policies and include the following:

- Employment practices
- Employee Standards of Conduct
- Conflict of Interest
- Performance Management
- Employee Discipline
- Information Security
- Corporate Communications
- Procurement and Contracts
- Records Management
- Asset Classification
- Workplace Security
- Business Continuity Planning

Corporate Policies



Corporate Organization

Corporate Policies

Employment

Employee Standards of Conduct

Conflict of Interest

Procurement and Contracts

Performance Management

Employee Discipline

Information Security

Corporate Communications

Workplace Security

Business Continuity Planning

Records Management

Asset Classification

FIGURE 4.1 Corporate Policies

Organization wide Policies

1. Employment

- This is the policy that describes the processes required to ensure that all candidates get an equal opportunity when seeking a position with the organization.
- This policy discusses the organization’s hiring practices and new employee orientation.
- The employment policies should also include condition-of-employment requirements such as background checks for key management levels or certain jobs.

2. Standards of Conduct

- This policy addresses what is expected of employees and how they are to conduct themselves when on company property or when representing the organization.
- Also included in this policy is a statement that “Company management has the responsibility to manage enterprise information, personnel, and physical properties relevant to their business operations, as well as the right to monitor the actual utilization of these enterprise assets.”

Organization wide Policies

3. Conflict of Interest

- Company employees are expected to adhere to the highest standards of conduct.
- To assure adherence to these standards, employees must have a special sensitivity to conflict-of-interest situations or relationships, as well as the inappropriateness of personal involvement in them.
- Many organizations restrict conflict-of-interest policy requirements to management levels; all employees should be required to annually review and sign a responsibility statement.

4. Performance Management

- This policy discusses how employee job performance is to be used in determining an employee's appraisal.
- Information security requirements should be included as an element that affects the level of employee performance.

Organization wide Policies

5. Employee Discipline

- This policy is very important for an effective information security program.
- When an investigation begins, it may eventually lead to a need to implement sanctions on an employee or group of employees.
- Having a policy that establishes who is responsible for administering these sanctions will ensure that all involved in the investigation are properly protected.

6. Information Security

- This is the cornerstone of the information security program and works in close harmony with the enterprise wide Asset Classification Policy and the Records Management Policy.
- This policy established the concept that information is an asset and the property of the organization, and that all employees are required to protect this asset.

Organization wide Policies

7. Corporate Communications

- Instead of individual, topic-specific policies on such items as voice-mail, e-mail, inter-office memos, outside correspondence, a single policy on what is and is not allowed in organization correspondence can be implemented.
- This policy will support the concepts established in the Employee Standards of Conduct, which address employee conduct and include harassment whether sexual, racial, religious, or ethnic.
- The policy also addresses requests from outside organizations for information.

8. Workplace Security

- This policy addresses the need to provide a safe and secure work environment for the employees.
- Included in this policy are the basic security tenets of authorized access to the facility, visitor requirements, property removal, and emergency response plans, which include evacuation procedures.

Organization wide Policies

9. Business Continuity Plans (BCPs)

Included in the Business Continuity Plan Policy are the needs for business units to:

- Establish effective continuity plans.
- Conduct business impact analyses for all applications, systems, and business processes.
- Identify preventive controls.
- Coordinate the business unit BCP with the IT disaster recovery plan.
- Test the plan and train its employees on the plan.
- Maintain the plan to a current state of readiness.

10. Procurement and Contracts

- This policy addresses those items that must be included in any contract, and this includes language that discusses the need for third parties to comply with organization’s policies, procedures, and standards.
- This policy is probably one of the most important for information security and other organization policies and standards.

Organization wide Policies

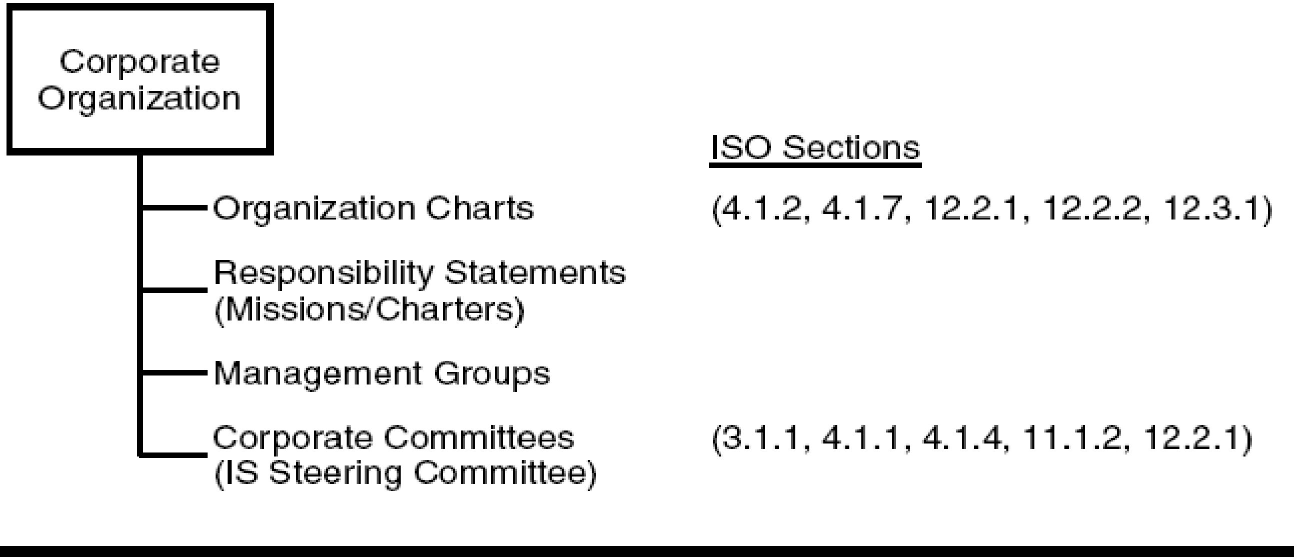
11. Records Management

- This policy normally establishes:
    - The record name
    - A brief description of the record
    - The owning department
    - The required length of time to keep the record

12. Asset Classification

- It normally includes the concepts of employee responsibilities, such as the Owner, Custodian, and User.
- The Asset Classification Policy adds:
    - The classification level
    - The owner’s job title

Organization wide Policy Document



Corporate Organization

	ISO Sections
Organization Charts	(4.1.2, 4.1.7, 12.2.1, 12.2.2, 12.3.1)
Responsibility Statements (Missions/Charters)	
Management Groups	
Corporate Committees (IS Steering Committee)	(3.1.1, 4.1.1, 4.1.4, 11.1.2, 12.2.1)

FIGURE 4.2 Corporate Policy Document

Legal Requirements

To perform two specific duties: **a duty of loyalty** and **a duty of care**.

Duty of Loyalty:

- By assuming office, senior management commits allegiance to the enterprise and acknowledges that the interest of the enterprise must prevail over any personal or individual interest.
- The duty of loyalty is evident in certain legal concepts:
    - Conflict of interest: Individuals must divulge any interest in outside relationships that might conflict with the enterprise's interests.
    - Duty of fairness: When presented with a conflict of interest, the individual has an obligation to act in the best interest of all parties.
    - Corporate opportunity: When presented with "material inside information" (advanced notice on mergers, acquisitions, patents, etc.), the individual will not use this information for personal gain.
    - Confidentiality: All matters involving the corporation should be kept in confidence until they are made public.

Duty of Care

- In addition to owing a duty of loyalty to the enterprise, the officers and directors also assume a duty to act carefully in fulfilling the important tasks of monitoring and directing the activities of corporate management.
- A director shall discharge his or her duties:
    - In good faith
    - With the care an ordinarily prudent person in a like position would exercise under similar circumstances
    - In a manner he or she reasonably believes is in the best interest of the enterprise

Federal Sentencing Guidelines for Criminal Convictions

1. The Federal Sentencing Guidelines define executive responsibility for fraud, theft, and antitrust violations, and establish a mandatory point system for federal judges to determine appropriate punishment.

There are seven elements that capture the basic functions inherent in most compliance programs:

1. Establish policies, standards, and procedures to guide the workforce.
2. Appoint a high-level manager to oversee compliance with the policies, standards, and procedures.
3. Exercise due care when granting discretionary authority to employees.
4. Assure compliance policies are being carried out.
5. Communicate the standards and procedures to all employees and others.
6. Enforce the policies, standards, and procedures consistently through appropriate disciplinary measures.
7. Establish procedures for corrections and modifications in case of violations.

The Economic Espionage Act of 1996

1. The Economic Espionage Act (EEA) of 1996 for the first time makes trade secret theft a federal crime, subject to penalties including fines, forfeiture, and imprisonment.
2. The act reinforces the rules governing trade secrets in that businesses must show that they have taken reasonable measures to protect their proprietary trade secrets in order to seek relief under the EEA.

The Foreign Corrupt Practices Act (FCPA)

1. For 20 years, regulators largely ignored the FCPA. This was due in part to an initial amnesty program under which nearly 500 companies admitted violations.
2. Now the federal government has dramatically increased its attention to business activities and is looking to enforce the act with vigor.

Sarbanes–Oxley (SOX) Act

Two important sections of the act are:

1. Section 302 (Disclosure Controls and Procedures or "DC&P") requires quarterly certification of financial statements by the CEO and CFO. The CEO and CFO must certify the completeness and accuracy of the filings and attest to the effectiveness of internal control.
2. Section 404 (Internal Control Attest) requires annual affirmation of management's responsibility for internal controls over financial reporting. Management must attest to the effectiveness based on an evaluation, and the auditor must attest to and report on management's evaluation.

Health Insurance Portability and Accountability Act (HIPAA)

1. The Health Insurance Portability and Accountability Act (HIPAA), also known as Kassebaum-Kennedy, after the two senators who spearheaded the bill.
2. The privacy and security rules within HIPAA govern the use, disclosure, and handling of any identifiable patient information by "covered" healthcare providers.
3. The law covers the information in whatever form it is seen or heard, and applies to the information in whatever manner it is to be used.

Gramm–Leach–Bliley Act (GLBA)

1. All financial services organizations must comply with GLBA data protection requirements. These requirements do not pertain only to providers receiving federal funds.
2. The GLBA requires financial institutions to:
3. Insure the security and confidentiality of customer records and information.
4. Protect against any anticipated threats or hazards to the security or integrity of such records.
5. Protect against unauthorized access.

Business Requirements

1. It is a well-accepted fact that it is important to protect the information essential to an organization, in the same way that it is important to protect the financial assets of the organization.
2. Unlike protecting financial assets, which have regulations to support their protection, the protection of information is often left to the individual employee.

Definitions

1. Policy:
    a. A policy is a high-level statement of enterprise beliefs, goals, and objectives and the general means for their attainment for a specified subject area.
    b. When we hear discussions on intrusion detection systems (IDS) monitoring compliance to company policies, these are not the policies we are discussing.
    c. The IDS is actually monitoring standards, which we will discuss in more detail later, or rule sets or proxies.

Standards

1. Standards are mandatory requirements that support individual policies.
2. Standards can range from what software or hardware can be used, to what remote access protocol is to be implemented, to who is responsible for approving what. We examine standards in more detail later in this book.

Procedures

1. Procedures are mandatory, step-by-step, detailed actions required to successfully complete a task. Procedures can be very detailed.

Guidelines

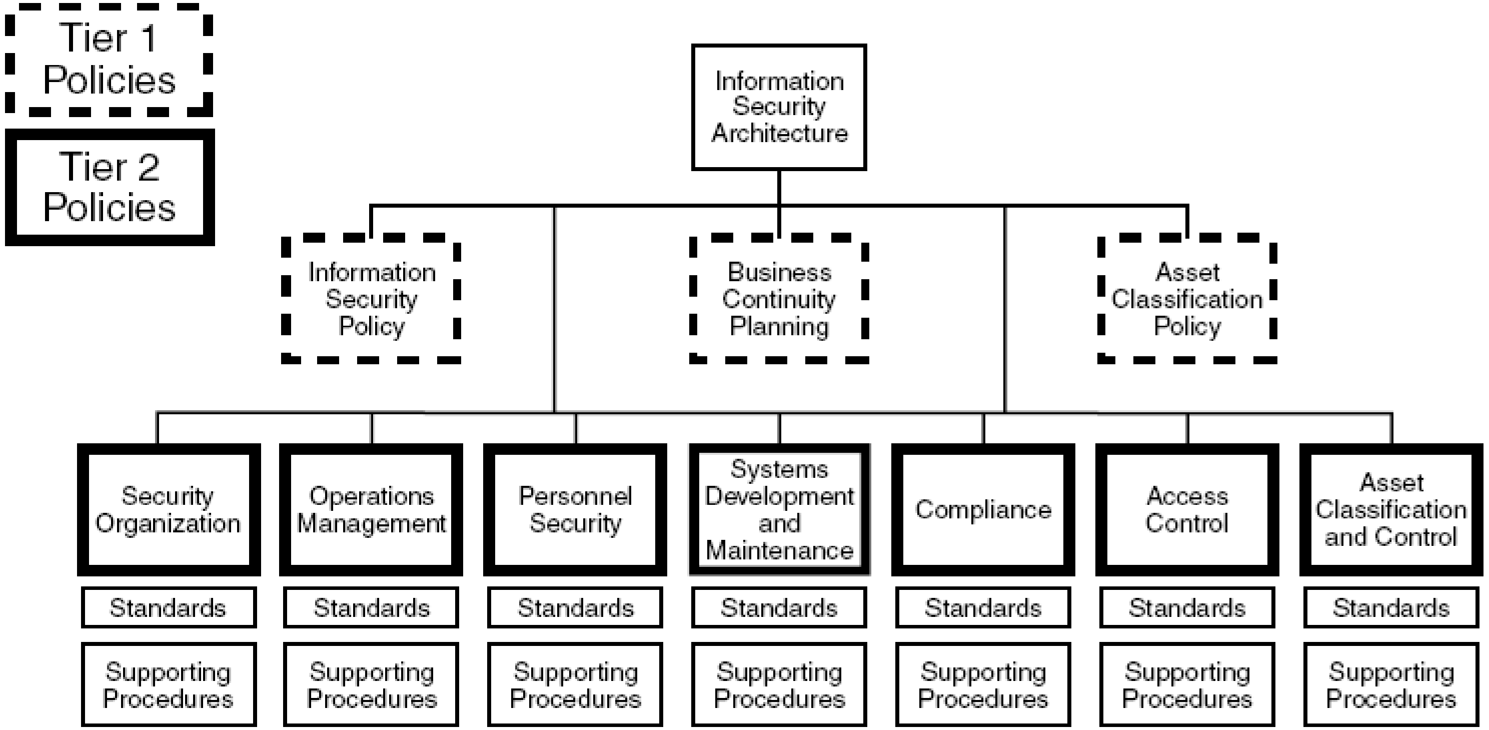
1. Guidelines are more general statements designed to achieve the policy's objectives by providing a framework within which to implement procedures.
2. Whereas standards are mandatory, guidelines are recommendations.

Policy Key Elements

1. The information security policy should cover all forms of information. In 1965, the computer industry introduced the concept of the "paperless office." The advent of third-generation computers had many in management believing that all information would be stored and secured electronically and that paper would become obsolete.

Policy Format

1. Policies are generally brief in comparison to procedures and normally consist of one page of text using both sides of the paper. In my classes I stress the concept of brevity.
2. However, it is important to balance brevity with clarity. Utilize all the words you need to complete the thought, but fight the urge to add more information.


Tier 1 Policies
Tier 2 Policies
Information Security Architecture
Information Security Policy
Business Continuity Planning
Asset Classification Policy
Security Organization
Operations Management
Personnel Security
Systems Development and Maintenance
Compliance
Access Control
Asset Classification and Control
Standards
Supporting Procedures

URE 4.3 Overall Information Security Policies and Standards Documents

The three types of policies are:

1. **Global (Tier 1)**. These are used to create the organization’s overall vision and direction.
2. **Topic-specific (Tier 2)**. These address particular subjects of concern.
3. **Application-specific (Tier 3)**. These focus on decisions taken by management to control particular applications (financial reporting, payroll, etc.) or specific systems (budgeting system).

Information security architecture

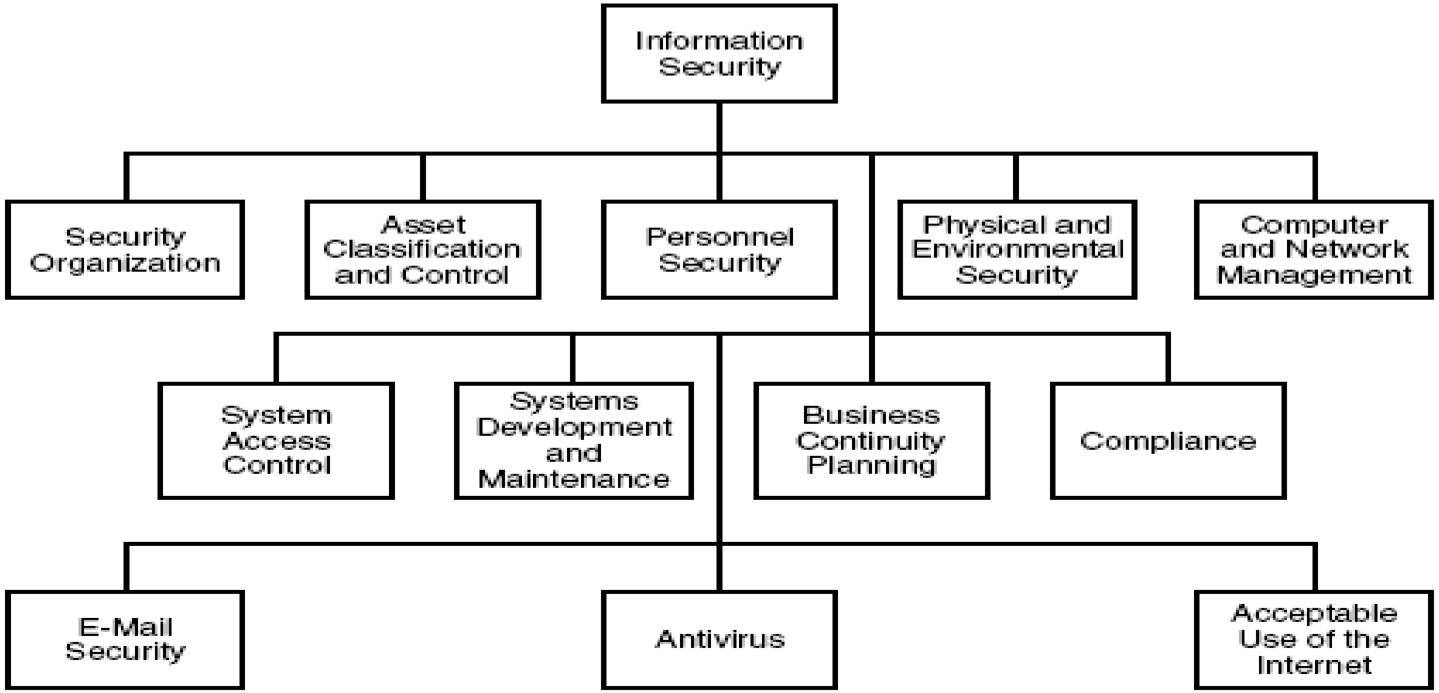

Information Security
Security Organization
Asset Classification and Control
Personnel Security
Physical and Environmental Security
Computer and Network Management
System Access Control
Systems Development and Maintenance
Business Continuity Planning
Compliance
E-Mail Security
Antivirus
Acceptable Use of the Internet

FIGURE 4.4 Topic-Specific (Tier 2) Policies

Global (Tier 1) Policy

1. An information security policy will define the intent of management and its sponsoring body with regard to protecting the information assets of the organization. It will include the scope of the program — that is, where it will reach and what information is included in this policy.
2. The components of a global (Tier 1) policy typically include four characteristics: topic, scope, responsibilities, and compliance or consequences.

Topic

1. The topic portion of the policy defines what specifically the policy is going to address. Because the attention span of readers is limited, the topic must appear quickly, say in the opening or topic sentence.
2. An opening topic sentence might read as follows: “Information created while employed by the company is the property of the company and must be properly protected.”

Scope

1. The scope can be used to broaden or narrow either the topic or the audience.
2. In an information security policy statement, we could say that “information is an asset and the property of the company and all employees are responsible for protecting that asset.”
3. In this sentence we have broadened the audience to include all employees.

Responsibilities

1. Typically, this section of the policy will identify who is responsible for what. When writing, it is better to identify the “who” by job title and not by name.
2. Here again, the Office Administrator’s Reference Guide can be of great assistance.
3. The policy will want to identify what is expected from each of the stakeholders.

Compliance or Consequences

1. When business units or employees are found in a noncompliant situation, the policy must spell out the consequences of these actions.
2. For business units or departments, if they are found in noncompliance, they are generally subject to an audit item and will have to prepare a formal compliance response.

Sample Information Security Global Policies

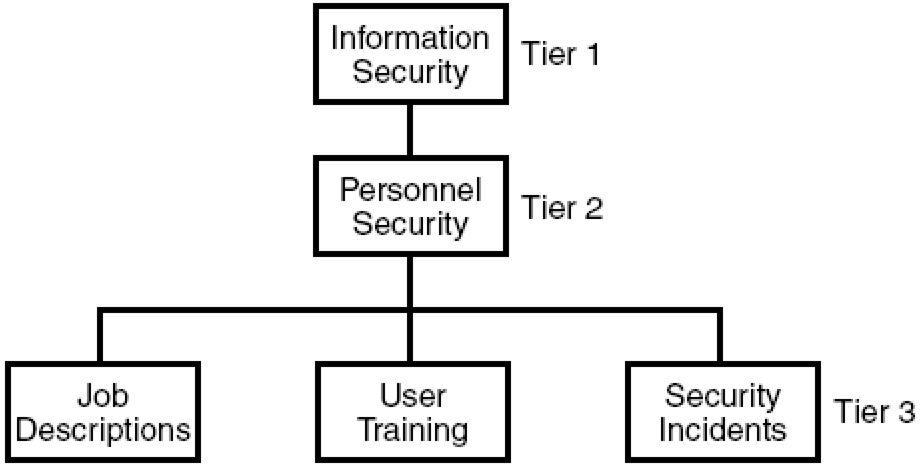
1. The written policy should clear up confusion, not generate new problems.
2. When preparing a document for a specific audience, remember that the writer will not have the opportunity to sit down with each reader and explain what each item or sentence means.
3. When writing a policy, know the audience. For a global (Tier 1) policy, the audience is the employee base.

Topic-Specific (Tier 2) Policy

1. Where the global (Tier 1) policy is intended to address the broad organization wide issues, the topic-specific (Tier 2) policy is developed to focus on areas of current relevance and concern to the organization.

Application-Specific (Tier 3) Policy

1. The application-specific (Tier 3) policy focuses on one specific system or application.
2. As the construction of an organization information security architecture takes shape, the final element will be the translation of Tier 1 and Tier 2 policies down to the application and system level.



Information Security

Tier 1

Personnel Security

Tier 2

Job Descriptions

User Training

Security Incidents

Tier 3

Thank you

The contents in this E-Material are from,

Thomas R. Peltier, Justin Peltier, John Blackley,
“Information Security and Fundamentals”,
Auerbach Publications, 2004