INFORMATION CLASSIFICATION AND INFORMATION HANDLING

BY,

JYOTHSNA.S

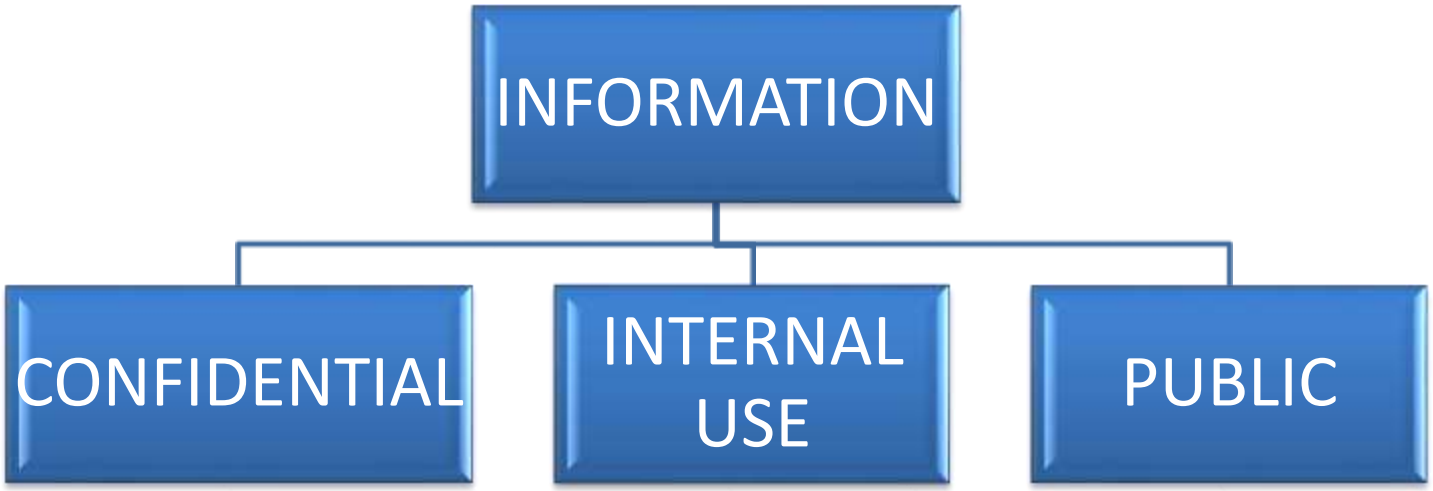
INFORMATION CLASSIFICATION

- Introduction
- Classification process
- Reclassification

INTRODUCTION

- Information, wherever it is handled or stored needs to be protected from unauthorized access, modification , disclosure, and destruction.

- Three basic classifications of information have been established.



CONFIDENTIAL DATA

- **DEFINITION:**

Information that, if disclosed, could:

- Violate the privacy of individuals.
- Reduce the company's competitive advantage
- Cause damage to the company.

- **EXAMPLES**:
  - Personnel records of individuals.
  - Customer information, shareholders information , vendor information
  - Specific operating plans, marketing plans, or strategies.
  - Specific business strategies and directions.
  - Major changes in the company's management structure

- **DISCUSSION:**

  - Information should be protected according to its sensitivity, criticality, and value.

  - It is estimated that approximately 5 to 15 percent of corporate information should be classified as Confidential.

  - Information regarded as sensitive should be labelled as Confidential.

INTERNAL USE

- **DEFINITION:**
  - Classify information as Internal Use when the information is intended for use by employees when conducting company business.

- **EXAMPLES:**
  - Operational business information and reports.
  - Non company information that is subject to a nondisclosure agreement with another company.
  - Company phone book.
  - Corporate policies, standards, and procedures.
  - Internal company announcements.

- DISCUSSION:

- This classification represents information that is used in the daily operation of the business and generally would not include planning or strategy development activities.

- It is estimated that 70 to 90 percent of corporate information can be classified as Internal Use.

- However, organizations such as customer accounting, legal, and personnel departments can be expected to have a larger percentage of Confidential information.

PUBLIC

- **DEFINITION:**
  - Classify information as Public if the information has been made available for public distribution through authorized company channels.
  - Public information is not sensitive in context or content, and requires no special security.
- **EXAMPLE:**

  The following are examples of Public information.
  - Corporate annual report.
  - Information specifically generated for public consumption, such as public service bulletins, marketing brochures, and advertisements.

- **DISCUSSION:**

- Generally, information that is readily available from the public media or is a matter of public record is classified as Public.

- It is estimated that 5 to 15 percent of corporate information can be classified as Public

CLASSIFICATION PROCESS

- **RECOMMENDED POLICY:**
  - The owner is responsible for classifying information upon creation.

- **DISCUSSION:**
  - Upon creation the creator of that information (generally the information owner) is responsible for immediate classification.
  - Information's value to the company is heavily influenced by the extent to which its integrity is maintained and is available to those with a business need.
  - The information owner must be careful not to over-classify information created.

RECLASSIFICATION

- **RECOMMENDED POLICY:**
  - The owner should review the classification of information at least annually for possible reclassification.

- **DISCUSSION:**
  - The sensitivity of most classified information decreases over time.
  - Confidential information may become Internal Use, and Internal Use may eventually become Public.
  - Because Confidential information often has a more restricted audience than Internal Use information, it is important that information be properly classified to give the widest and most appropriate audience possible

INFORMATION HANDLING

- Introduction
- Information labelling
- Information use and duplication
- Information storage
- Information disposal

INTRODUCTION

- Information handling will help to identify standards and guidelines to help safeguard information during its useful life.
- This process will take place once the information is obtained and classified.

INFORMATION LABELING

- **RECOMMENDED STANDARD:**

  - All Confidential information must be clearly labeled with the word "Confidential." Any information not specifically labelled should be treated as Internal Use

RECOMMENDED PROCEDURE:

All Confidential information is to be marked as follows:

- The name of the owner and the date of preparation are to appear on the face of the document.
- The document or any reproduction is to be stamped or marked Confidential at the top of the outside cover (if applicable) or on the title page.
- Only Confidential information requires labelling. Public information should be labeled to identify its intended audience. Information not labeled should be protected as Internal Use.

INFORMATION USE AND DUPLICATION

- **RECOMMENDED STANDARD:**
  - Information for which access has been authorized may only be used for purposes identified to and authorized by the information owner.
- **DISCUSSION:**
  - When the information owner provides access to information, it is authorized on the basis of the requester's established business need.
  - Access to information is approved for a stated purpose and does not imply that the requester has unrestricted use or authority to use for other purposes.
  - Sometimes the authorization given by the information owner to the user needs to be formal and written or can be verbal too.

INFORMATION STORAGE

- **CORPORATE POLICY**:
  - Organizations shall retain records in the most economical and practical method and location, and shall destroy or relocate them to more economical storage when appropriate.
- **RECOMMENDED STANDARD:**

Information must be stored in a manner consistent with its classification as follows:

- When not in use, information is to be appropriately stored.
- Confidential information is to be stored and maintained only where it can be verified that access can be adequately controlled.

- **DISCUSSION:**

  - Information, particularly Confidential information, must be safeguarded not only while in use, but also when stored to protect against unauthorized access, modification.

  - This may mean that paper-based information may need to be stored in locked cabinets or desks while not in use.

  - For computer based information, this may mean physically locking the computer while not attended by an authorized individual or installing an access control software package to protect against unauthorized access.

INFORMATION DISPOSAL

- **CORPORATE POLICY:**
  - Organizations shall retain records in the most economical and practical method and location, and shall destroy or relocate them to more economical storage when appropriate.
- **RECOMMENDED STANDARD:**
  - Information must be appropriately destroyed in accordance with the organization's records retention schedule.
  - Information no longer of value to the company should be destroyed.
  - Confidential information must be destroyed beyond ability to recognize and recover.

- DISCUSSION:
  - When the information no longer has value to the user, his or her copy of the information should be destroyed.
  - When the information no longer has value to the company, the information owner is responsible for disposal of the information originals.
  - For Internal Use information, this might mean simply throwing the report in the trash or deleting the file from the computer.
  - For Confidential information, however, additional care is necessary to ensure that the discarded information can-not be recognized or recovered by anyone.
  - Owners and users also need to ensure that all data backups of the information are also destroyed beyond recovery.

Information Security Program Administration

- Publishing a set of policies and procedures is no assurance that anyone will ever read them.
- Creating an employee awareness program is necessary to bring the information security message to all employees.
- Before employees can accept an Information Security (IS) program, they must first understand why the program is necessary and what they will gain from its implementation.
- To facilitate this process, a structure has been established to administer the program, its direction and scope .

CORPORATE INFORMATION SYSTEMS STEERING COMMITTEE

- This committee, consisting of senior management who will share about the available and emerging information technologies to improve efficiency and effectiveness to meet the competitive challenges that lie ahead.

- This group has approved and supports the vision and goals of the Information Security program.

- They provide guidance, ensuring that the program is consistent with company goals, measures, and targets.

- They ensure the availability of resources necessary for successful implementation and maintenance of the program.

CORPORATE INFORMATION SECURITY PROGRAM

- **Corporate Information Security Manager**:

- This individual will support and direct the corporate Information Security program.
- This will be accomplished by ensuring that necessary resources are available.

Corporate Information Security Coordinator

- This individual is responsible for maintenance of the program's vision, goals, and elements, and for proposing necessary changes to the IS Steering Committee for approval.
- This individual will train and coordinate the organization IS coordinators, supporting them with regular contact, information security awareness tools, consultation, and ideas.
- To ensure progress throughout the IS program life cycle, this individual will monitor each organizational unit's progress and keep the Corporate IS Manager updated.

ORGANIZATION INFORMATION SECURITY PROGRAM

- Organization Management

They will be asked to promote the program by providing appropriate staff and other resources to ensure security of corporate information assets. It is crucial that they also support their organization IS coordinators in the development and maintenance of a local information security program.

- Information Security Coordinators :

Organization Coordinators:An Organization Information Security Coordinator is appointed by organization management to develop, implement, and maintain an organization IS program consistent with corporate and organization objectives

Group Coordinators (Optional):Group Information Security Coordinators assist the Organization IS Coordinator in large organizations.

- Area Coordinators (Optional):

Area Information Security Coordinators assist the Group IS Coordinator in large groups within an organization.

Area IS Coordinators are appointed by the management of areas within a group to perform area-level duties that support the organization IS program.

These individuals should perform area-level information risk assessments and may meet with area personnel to build their awareness of information security issues.

THANK YOU