## Information Classification

### Introduction

- After identifying the information to be protected, it is necessary to classify the information and organize it according to its sensitivity to loss, disclosure or unavailability.
- The primary purpose of data classification is to indicate the protection level of confidentiality, Integrity and Availability required for each type of dataset.
- Data classification helps to ensure that the data is protected in the most cost-effective manner.
- Each classification should have separate handling requirements and procedures pertaining to how that data is accessed, used, and destroyed.

### Classification Types

| Classification | Definition | Examples | Organization That Would Use This |
|---|---|---|---|
| Public | • Disclosure is not welcome, but it would not cause an adverse impact to company or personnel. | • How many people are working on a specific project<br>• Upcoming projects | Commercial business |
| Sensitive | • Requires special precautions to ensure the integrity and confidentiality of the data by protecting it from unauthorized Modification or deletion.<br>• Requires higher than normal assurance of accuracy and \|completeness. | • Financial information<br>• Details of projects<br>• Profit earnings and forecasts | Commercial business |
| Private | • Personal information for use within a company.<br>• Unauthorized disclosure could adversely affect personnel. or company | • Work history<br>• Human resources information<br>• Medical information | Commercial business |

| | | | |
|---|---|---|---|
| Confidential | • For use within the company only.<br>• Data that is exempt from disclosure under the Freedom of Information Act or other laws and regulations.<br>• Unauthorized disclosure could seriously affect a company. | • Trade secrets<br>• Health care information<br>• Programming code<br>• Information that keeps a company competitive | Commercial business / Military |
| Unclassified | • Data is not sensitive or classified. | • Computer manual and warranty information<br>• Recruiting information | Military |
| Sensitive but unclassified (SBU) | • Minor secret.<br>• If disclosed, it could cause serious damage. | • Medical data<br>• Answers to test scores | Military |
| Secret | • If disclosed, it could cause serious damage to national security. | • Deployment plans for troops<br>• Nuclear bomb placement | Military |
| Top secret | • If disclosed, it could cause grave damage to national security. | • Blueprints of new wartime weapons<br>• Spy satellite information<br>• Espionage data | Military |

**Guidelines for Information Classification**

- The classification should neither be a long list nor be too restrictive and detailed-oriented.
- Each classification should be unique and should not have any overlapping.
- The classification process should outline how information and applications are and handled throughout their life cycle.

## Criteria for Information Classification

- Usefulness of data
- Value of data
- Age of data
- The level of damage that could be caused if the data were disclosed
- The level of damage that could be caused if the data were modified or corrupted
- Legal, regulatory, or contractual responsibility to protect the data
- Effects the data has on national security
- Who should be able to access the data
- Who should maintain the data
- Where the data should be kept
- Who should be able to reproduce the data
- What data requires labels and special marking
- Whether encryption is required for the data
- Whether separation of duties is required
- Which Backup Strategy is appropriate
- Which Recovery Strategy is appropriate

**Security Note**: An organization needs to make sure that whoever is backing up classified data--and whoever has access to backed-up data--has the necessary clearance level.
A large security risk can be introduced if low-end technicians with no security clearance can have access to this information during their tasks. Backups contain all your data and deserve the same considerations in terms of security risk as the entire infrastructure because that is exactly what it is only in a single location, often stored as a single file and usually with little thought put into what are the risks involved with that appliance.

## Data Classification Procedures

The following outlines the necessary steps for a proper classification program:

- Define classification levels.
- Specify the criteria that will determine how data is classified.
- Have the data owner indicate the classification of the data she is responsible for.
- Identify the data custodian who will be responsible for maintaining data and its security level.

- Indicate the security controls, or protection mechanisms, that are required for each classification level.
- Document any exceptions to the previous classification issues.
- Indicate the methods that can be used to transfer custody of the information to a different data owner.
- Create a procedure to periodically review the classification and ownership. Communicate any changes to the data custodian.
- Indicate termination procedures for declassifying the data.
- Integrate these issues into the security-awareness program so that all employees understand how to handle data at different classification levels.

**Classification Controls**

The type of control implemented per classification depends upon the level of protection that management and the security team have determined is needed. Some of the controls are :

- Strict and granular access control for all levels of sensitive data and programs
- Encryption of data while stored and while in transmission
- Auditing and monitoring (determine what level of auditing is required and how long logs are to be retained)
- Separation of duties (determine whether two or more people need to be involved in accessing sensitive information to protect against fraudulent activities; if so, define and document procedures)
- Periodic reviews (review classification levels, and the data and programs that adhere to them, to ensure that they are still in alignment with business needs; data or applications may also need to be reclassified or declassified, depending upon the situation)
- Backup and recovery procedures (define and document)
- Change control procedures (define and document)
- File and file system access permissions (define and document)