

Security Management Data Classification

- ❖ *DigitalSherlock.com | SafeHack.com*
- ❖ *Date: 2005/05/27*
- ❖ *Document Name: security_management_data_classification.pdf*
- ❖ *GNU Free Documentation License*
- ❖ *Version 1.00, 2005-05-27*
- ❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*
- ❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

❖ Objectives

- **We classify information in order to determine the appropriate level of protection required**
- **Primary purpose to enhance confidentiality, integrity, and availability**
- **Has a higher enterprise level benefit**
- **There shouldn't be too many categories as this will make it hard for the person classifying the information**
- **Classified information is generally government information**
- **Labels are used to identify the classification/categorization that is attached to an object or subject**

❖ Benefit

- **Demonstrates an organization's commitment to security protections**
- **Help identify which information is the most sensitive or vital to an organization**
- **Supports the tenets confidentiality, integrity, and availability**
- **Help identify which protections apply to which information**
- **May be required for regulatory, compliance, or legal reasons.**

❖ GOV Sector

- **Unclassified**
 - **Data is not sensitive or classified**
 - **The public release of this information DOES NOT violate confidentiality**
 - **Example**
 - Computer manual
 - Warranty information
 - Recruiting information
- **Sensitive but Unclassified (SBU)**
 - **Minor secret**
 - **Unauthorized disclosure COULD cause SERIOUSE damage**
 - **May NOT create serious damage if diclosed**
 - **Example**
 - Health care data
 - Answers to test scores
- **Confidential**
 - **Information designated confidential nature**
 - **Unauthorized disclosure COULD cause some damage to the COUNTRY**

➤ **Secret**

- **Unauthorized disclosure COULD cause SERIOUSE damage to the country**
- **Example**
 - Troops deployment plans
 - Nuclear bomb placement

➤ **Top Secret**

- **The highest level of information**
- **Unauthorized disclosure cause EXCEPTIONALLY GRAVE damage to the country**
- **Example**
 - Blueprint of new wartime weapons
 - Spy satellite information
 - Espionage Data

➤ **President Of USA**

- **The president of USA has a level only for him**

❖ **Public Sector**

➤ **Proprietary**

- **If disclosed it could reduce competitive edge**
- **Example**
 - Recipe to soft drink or trade secret
 - Technical specifications

➤ **Public**

- **All data that does not fit into previous classes**
- **Disclosure is not welcome, but it would not cause an adverse impact to company or personnel**
- **Example**
 - Upcoming Event
 - Upcoming Projects
 - How many peoples are workingon a specific project

➤ **Private**

- **Information considered of a personal nature**
- **Intended for company use only**
- **Disclosure COULD Adversely affect the company or personnel**
- **Example**
 - Example Salary, Medical information

➤ **Confidential**

- **Information very sensitive**
- **Intened for INTERNAL use only**
- **Exempt from disclosure under the Freedom of Information Act**
- **Disclosure COULD SERIOUSLY affect the company**
- **Example Info about new product, Trade secrets, merger negotiations**

➤ **Sensitive**

- **Require higher level of classification than normal data**
- **This information is protected from a loss of confidentiality as well as integrity**

❖ **Classifications criteria**

- **Value**
 - Number ONE commonly used to classify data in PUBLIC sector
 - If the information is valuable it need to be classified
 - What is this information worth to the company?
 - How much would it cost to reproduce if it was lost?
- **Age**
 - The classification may be lowered if the information value decreases over time
 - How old is this information?
 - When will it's useful lifetime be reached?
- **Useful Life**
 - The information made obsolete due to new information
 - Example: Substantial change in the company
- **Personal Associations**
 - If information is personally associated with specific individuals
 - Example: Investigation information that reveals nams may need to remain classified
- **Authorization**
 - Who is authorized to see this information?
 - Who is authorized to allow declassification?
- **Custody**
 - Who will have custody of this information?
 - How will they determine if the requesting user is entitled access?
- **Reproduction**
 - Can this material be copied?
 - If so, how will distribution be controlled?
- **Logging Should records be kept regarding**
 - Who has the material
 - Was it returned or destroyed?
 - Was it copied?
- **Marking and Labeling**
 - How will the classified information be labeled and marked to show the classification?
 - How will the information be protected in storage?
 - Does it requires the use of encryption or special locking mechanisms?
- **Filing and Safekeeping**

❖ **Classifications Procedures**

- Identify the administrator/Custodian
- Specify the criteria of how the information will be classified and labeled
- Classify the data by its owner
- Specify and document any exceptions to the classification level
- Specify the controls that will be applied to each classification level
- Specify the termination procedures for declassifying the information
- Create an entreprise awareness program about classification controls

❖ **Roles**

➤ **Owners**

- Management is responsible for protecting all assets that are directly or indirectly under their control
- Executive or manager of an organization
- This person is responsible for the asset of information
- Has the final corporate responsibility of data protection
- Liable for negligence
- Responsibilities include

➤ **Custodian**

- Custodian is delegated the responsibility of protecting the information by its owner
- This role is commonly executed by IT system personnel
- Responsibilities include

➤ **User**

- Any employees
- Contractors
- External party
- Responsibilities include