HPOL#02
Asset Classification and Control

(Version 1.0)

Table of Contents

2.1. SCOPE AND OBJECTIVES

The government organizations are committed to protect its information assets. In order to determine the level of protection required, and to ensure that integrity and confidentiality of information is maintained, the information assets require to be identified, and a data classification scheme should be designed.

This policy document addresses security issues related to information assets with regard to information asset inventory, information asset classification, handling and labeling of information.

The level of security to be afforded to the information will depend directly on the classification of the data. All employees, especially those who may come into contact with "sensitive" information are expected to familiarize themselves with this data classification scheme, and to consistently use it in the activities of the organization.

2.2. POLICY STATEMENT

2.2.1. RISK ASSESSMENT

2.2.1.1. Risk Assessment Process

2.2.1.1.1. A risk assessment process should be established that addresses the sensitivity and the criticality of information.

Explanatory Notes

The process of risk assessment should take into consideration the following:

- *Sensitivity of Information - The degree to which the value of the information is determined by its secrecy.*
- *Criticality of Information – Criticality is comprised of two components, Integrity and Availability. Integrity Criticality is the degree to which the value of the information is determined by its reliability. Availability Criticality is the degree to which the value of the information is determined by its accessibility when needed.*

2.2.2. ASSET CONTROL

2.2.2.1. Need to Know

2.2.2.1.1. An asset classification scheme should be designed to support the “need to know” policy so that information will be protected from unauthorized disclosure, use, modification, and deletion.

Explanatory Notes

One of the fundamental principles of information security is the "need to know." This principle holds that information should be disclosed only to those people who have a legitimate business need for the information.

2.2.2.2. Consistent Protection

2.2.2.2.1. Information must be consistently protected throughout its life cycle, from its origination to its destruction.

Explanatory Notes

Information must be protected in a manner commensurate with its sensitivity, no matter where it resides, what form it takes, what technology was used to handle it, and what purpose it serves.

2.2.2.3. Asset Protection Scheme

2.2.2.3.1. Asset Protection should include the classification of the asset to be protected and the implementation of labeling, handling, and destruction procedures according to the asset's classification.

<u>Explanatory Notes</u>

Asset Protection is the process of defining controls to effectively protect an information asset.

2.2.3. ASSET CLASSIFICATION

2.2.3.1. Information Systems Asset Inventory

2.2.3.1.1. The assets of the government organization must be listed in an information asset inventory.

<u>Explanatory Notes</u>

Each asset must be clearly identified individually and (if appropriate) collectively in combination with other assets to form an identifiable information system.

2.2.3.1.2. Each information asset must have a nominated owner.

<u>Explanatory Notes</u>

The information asset owner has the responsibility of classifying the asset on the basis of the asset classification scheme and related guidelines of the government organization.

2.2.3.1.3. The owner of the information asset must identify / approve of the controls that should be implemented to provide appropriate protection to the asset.

<u>Explanatory Notes</u>

The owner of the information asset is accountable for the security of the information asset.

2.2.3.1.4. Each information asset must also have a nominated custodian.

Explanatory Notes

The custodian may be separate from the 'owner' of the information asset. The custodian of the information asset will be responsible for the protection of the asset and for implementing the controls (as identified and approved by the owner of the information asset) related to the protection of the asset.

2.2.3.2. Information Asset Classification

2.2.3.2.1. Information assets must be classified in accordance with a specific asset classification scheme and related guidelines to be developed for this purpose.

Explanatory Notes

Data contained within an information system (master data, data under process, etc.) and the output from information systems assets will also derive its classification label based on the asset classification scheme and associated guidelines of the government organization.

2.2.3.2.2. The classification of each information asset is to be reviewed at periodic intervals and may be amended in accordance with the asset classification scheme and related guidelines in force at the time.

2.2.3.3. Handling and Labelling of Information

2.2.3.3.1. All information assets shall be labeled physically or electronically in accordance with their asset classification.

Explanatory Notes

Information assets will be maintained, handled, stored, transported (or transmitted) or destroyed in accordance *with the data handling procedures associated with the asset's classification label.*

2.2.3.4. Asset Classification Criteria

2.2.3.4.1. Information assets will be assigned classifications based on their susceptibility to risk.

Explanatory Notes

Risk classification will enable the government organizations to focus asset protection mechanisms on those assets that are most susceptible to specific risks.

Criteria for asset classification should include but not be limited to:

- *Confidentiality - Confidentiality criteria define the level of secrecy to be accorded to the information assets and consequently the level of accessibility to the information it contains or represents.*

- *Integrity - Integrity of information relates to the impact of unauthorized modification to an information asset or loss of the information asset or data contained therein.*

- *Availability - Availability criteria relates to the impact of an information asset being unavailable. Availability criteria are further subdivided into long-term unavailability and short-term unavailability.*

2.2.3.5. Declassification / Downgrading

2.2.3.5.1. The designated information asset owner may, at any time, declassify or downgrade information.

Explanatory Notes

To achieve this, the owner must change the classification label appearing on the original document and notify all known recipients / users.

2.2.3.5.2. If known, the date that restricted or confidential information will no longer be sensitive (declassified) must be indicated on all sensitive information.

2.2.3.5.3. The designated information asset owner may, at any time prior to scheduled declassification or downgrading, extend the period that information is to remain at a certain classification level.

2.2.3.5.4. To determine whether sensitive information may be declassified or downgraded, information asset owners must review the sensitivity classifications assigned to information for which they are responsible, on a periodic basis.