Information Classification and Handling Guideline

Document No: ISMS03-0006

Version 1.0

Published Date：03/23/2020

Table of Contents

Version Control Log

Version	Date	Changes Included	Organization	Author	V&V
1.0	03/23/2020		DOT	Doc Team	Director

1. Purpose

To ensure that information receives an appropriate level of protection in accordance with its importance to the organization. Classifying and labelling of the information in accordance to the value, criticality and sensitivity of the data, and properly disposing of the media used to store them.

2. Scope

Applicable to all operations, staff, and users of the Department of Technology (DOT) business process.

3. Definition

Project

A temporary task that has initiating and closing dates during which progressive elaboration takes place, and produces a unique product, service, or process at the end.

4. Responsibility

4.1 Management

4.1.1 Management should conduct periodical scheme assessment every 3 months and de-sensitize information when information is deemed non-confidential.

4.1.2 Approval or dismissal of disposal procedures.

4.1.3 Enforce approved disposal procedures.

4.1.4 Receive notification upon completion of disposal execution.

4.2 Coordinators

4.2.1 Coordinators are responsible for the proper disposal of media related to services and systems managed by DOT.

4.2.2 Coordinators must adhere to the proper disposal procedures and must garner approval from Director for alternate methods not outlined in this document.

4.2.3 Director should approve disposal methods of media.

4.2.4 Properly notify and alert other Administrators to disposal of media

4.3 Administrators

4.3.1 The Administrator are directly responsible for receiving, unpacking, storing and shipping of all equipment coming in and out of the DOT building.

4.3.2 The Administrators are responsible for security of all network devices at the main office and at remote locations.

4.3.3 The Administrators are responsible for security and usage regulations for all Servers, NAS System etc.

4.4 All staff

All staff should be familiar with and follow the guideline of information classification, labelling, handling and assets disposal.

5. Content

5.1 Information Classification

Information may include organizational documents, procedures, policies, operational plans, charters, reports, database contents etc., it can be contained on media of any form. Information used in projects is also within the scope of the information described above and needs to follow the information classification scheme within DOT business process. Examples of project information are supplier contracts, Non-Disclosure Agreements, statement of work, work breakdown structure, deliverables etc.

Information classification is of the highest priority at the DOT. This document outlines the classification scheme utilized to determine the category that the different types of information belong to and the associated labelling process and procedure respectively. Furthermore, procedures for asset handling are present to ensure the confidentiality, integrity and availability of the defined categories. All staff of the DOT business process should follow the schemes specified in this document.

5.1.1 Information Classification Scheme

5.1.1.1 Public – information that is readily available to DOT and any entities outside DOT.

5.1.1.2 Internal – information accessible by staff within DOT business process.

5.1.1.3 Confidential – information accessible by only specific groups or members within DOT business process, including but not limited to any information related confidential matters, e.g. budget planning, project plan, network plan, firewall policy, password table, and encryption key.

5.1.1.4 Extremely Confidential – information accessible only by restricted persons, including but not limited to any information related human resource matters, privacy or personal information.

5.2 Information Labelling

This section documents the set of procedures necessary in order to label the information based on the defined Classification Scheme. The labelling process for information is to be wholly reflective of the category in which they are placed based on the below schema.

5.2.1 Labels

The labels should reflect the determined level of security and potential threat associated to the information assets. Labels exist such that members of the department should be able to identify the standards and procedures necessary to handle information assets based on the given label.

5.2.1.1 Public - the "Public" label is given to provide information wherein the disclosure or destruction of that data would result in no risk to the organization. Example: brochures for the main office building or aggregated information for public use.

5.2.1.2 Internal - the "Internal" label is given to provide information wherein the unauthorized disclosure, alteration or destruction of that data would result in a small or limited adverse effect(s) on the organization. Example: the location area where all public forms are available.

5.2.1.3 Confidential - the "Confidential" label is given to provide information wherein the unauthorized disclosure, alteration or destruction of that data would result in significant adverse impact(s) on the organization. Example: Passwords for privileged accounts.

5.2.1.4 Extremely Confidential - the "Extremely Confidential" label is given to provide information wherein the unauthorized disclosure, alteration or destruction of that data would result in significant adverse impact(s) on the organization. Example: personal information.

5.2.2 Labelling of Information Assets

5.2.2.1 Workstation Labelling

(1) First a naming scheme has to be chosen (WSXXXXXX).

(2) The naming scheme is chosen depending of the Ministry and location of the new workstation.

(3) Then identify if the workstation is a replacement or if it is a new machine on the network.

(4) If the machine is a replacement:

A Identify the computer name of the machine being replaced.

B Use the same computer name identified and assign it to the new workstation with a "T" at the end of the computer name.
Note: This temporary "T" on the computer name is removed after the old machine has been replaced with the new one.

(5) If the machine is a new machine on the network, the next available computer name is used as the computer name or any other name that might have been skipped.

5.2.2.2 Cable labelling

Network cables are labelled according to the same naming scheme used for a PC within a certain location or according to the switch position.

5.2.2.3 Printer Labelling

The printers follow the same naming scheme that is being used within a certain location or unit it is located in, just that in this case a PR for Printer is attached to the front of the name. (PRINTER Unit) Note: WS (WorkStation), PR (Printer), NC (Network Cable). Ex. PR Tech.

5.3 Information Handling

5.3.1 Internal category

5.3.1.1 Written documents

(1) It should be stored with proper preservation to prevent from being viewed or taken by extremal parties.

(2) Do not leave any unattended copy on the machine while scanning, printing, photocopying or faxing.

5.3.1.2 Storage media

(1) Keep desktop clear, remove any storage media (e.g. diskette, CD) from desktop when unattended for a long period of time (e.g. more than 15 minutes).

(2) When it is to be disposed or no more useable, the content should be erased or the media contains the information should be destroyed.

5.3.1.3 Electronic files

(1) Always activate screen saver when leaving PC unattended. Shutdown the PC

after office hour unless otherwise instructed for specific purposes.

(2) Electronic files should be password protected to prevent from being viewed or taken by irrelevant personnel.

(3) Electronic files should be password protected if it's to be transferred through external or public network.

5.3.2 Confidential category

5.3.2.1 Written documents

(1) Store

A Documents should be stored in locked container or control area to avoid from being viewed or taken. They should be accessed by authorized personnel and should not be used in public place.

B Documents should not be left on desktop when unattended or after office hour.

(2) Transfer

A When documents are transferred internally, they should be transferred by designated or authorized persons.

B Documents should not be left unattended on machines while scanning, printing, photocopying or faxing.

C Documents should not be sent by mail to external parties unless they are registered mail or by designated persons.

D Documents containing personal information should be transferred in person. The name, signature of the person, time and destination should be registered. While transferring personal information to outsourced vendors, register date, quantity, purpose and recipient should be documented.

(3) Retrieval

Retrieving Confidential information by staff not responsible for the business should be approved by the manager or authorized personnel (with information ownership). The retriever and time should be documented.

(4) Destruction

A Reuse is not allowed. Documents should be destroyed by shredder.

B When disposing a large number of documents, they should be packed with seal affixed and located in a safe place before destruction.

C Designated personnel should participate in transit of document to site of destruction, supervise the destruction and keep the evidence.

5.3.2.2 Storage media

(1) Store

A Label the confidentiality level on the media. Use red sticker or hand writing on diskette, CD or tapes etc.

B Media should be stored in locked container or control area to avoid from being viewed or taken by irrelevant person.

C Media should not be left on desktop or machine when unattended for 1 hour or after office hour.

(2) Transfer

A When transferred internally, media should be transferred in person or by authorized persons.

B When sent by mail to external party, media should be sent through registered mail or by designated person.

C While transferring storage media (such as hard drive, tape, USB flash drive) which contains personal information, a designated person should be assigned and to document media number (e.g. tape number), signature of designated person, time and destination.

D While transferring storage media that contains personal information by external parties (e.g. post office, express delivery vendor), strong packaging should be used, and relevant records should be retained.

E While transferring personal information through email to outsourced vendors, date, quantity, purpose and recipient information should be documented.

(3) Retrieval

Retrieving information by staff not responsible for business should be approved by the manager or authorized personnel (with information ownership). The retriever and time should be documented.

(4) Destruction

A Before scrapping or transferring for other usage, information in the media should be erased or the media should be formatted.

B Use shredder, degauss or physical damage mechanism to securely destroy the media.

C Storage media, servers or equipment should be degaussed or physically damaged.

5.3.2.3 Electronic files

(1) Store

A Always activate screen saver when leaving PC unattended. Shutdown the PC

after office hour unless otherwise instructed for specific purposes.

B The key should have a backup copy to avoid damage of the key when encryption is used to protect files or folders. The backup key should be preserved properly and only accessed by authorized person.

C Personal information files should be encrypted, they are not allowed to store in share folder, private own mobile device (e.g. USB flash drive, laptop, tablet, mobile phone, digital camera and record pen) or mobile device without custodian.

D The place storing personal information files should have physical control such as access control, lock drawer and access control of users.

(2) Transfer

A Data Copy, removal or transmission should be authorized and only sent to authorized recipient.

B When transferring electronic files with password protection or encryption, the password or key should be protected and transmitted to the recipient through another email or via a different method. Password should not be sent in same email.

(3) Retrieval

Retrieving Confidential information by staff not responsible for the business should be approved by the manager or authorized personnel (with information ownership). The retriever and time should be documented.

(4) Deletion

A If the retention period expired or files are no longer in use, they should be deleted and removed from Recycled Bin.

B When needed, software tools can be used to ensure deleted files are not able to recover.

5.4 Information Assets Handling

5.4.1 After assets have been placed in storage, they are immediately logged and inventoried by the Administrator and the information is shared with the Senior Executive Officer.

5.4.2 After the equipment have been carefully stored and put on the inventory list, the Administrators/Technicians are responsible to disseminate the equipment to departments if necessary.

5.4.3 Department representative must fill out the “ISMS04_0024_Service Request Form” and the “ISMS04_0025_Equipment Removal Log Sheet” when requesting to remove the equipment from the server/storage room.

5.4.4 External users are required to sign a contract (see “ISMS04_0026_Employee Laptop

Agreement" and "ISMS04_0027_ Toolkit Agreement for Technical Staff") accepting responsibility for the equipment if needed for personal use (laptops and tool kits).

5.4.5 The server/storage room is always kept locked and is only accessible by authorized personnel. All network equipment that has been disseminated to the network team to set up at remote locations are locked in a storage room and the keys are kept by the Coordinators. In the event personnel need to use equipment, an authorized person should access the storage room to retrieve the equipment needed, all critical equipment that is required for system administration is stored in the server/storage room.

5.5 Information Assets Disposal

5.5.1 Physical Destruction of Storage Media

Step 1 - Determine what media is to be disposed.

Step2 – Receive approval from the Director, all storage media are collected and accounted for. Media containing sensitive information that can be used later is set aside for archiving. They are stored in a secure location only known to authorized personnel and the Director.

Step3 – At the specified time, designated personnel should begin the process of physically breaking the storage media.

5.5.2 Hard drive disposal

5.5.2.1 Before the hard drive disposal process, all sensitive data and licensed software installed in the equipment should be removed.

5.5.2.2 Hard drive should be formatted (write zeroes, low level format) completely before disposal.

5.5.3 Paper Files Destruction Process

Step 1 - Assess and determine what physical documents to be disposed.

Step2 – Schedule time and location of disposal with the approval of the Director if the content is deemed confidential.

6. Reference

None

7. Form

ISMS04_0024_Service Request Form

ISMS04_0025_Equipment Removal Log Sheet

ISMS04_0026_Employee Laptop Agreement

ISMS04_0027_Toolkit Agreement for Technical Staff