Information Transfer Policy

Document No: ISMS03-0005

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 and maintain the security of information transferred within DOT and with any external entity.

2. Scope

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

3. Definition

3.1 PSO

Public Service Orders

3.2 Confidential and/or restricted information

Applies to DOT business process or management related information which is strictly accessible by authorized groups or members.

3.3 VPN

Virtual Private Network is a method use to securely provide network service to the remote sites.

3.4 FTP

File Transfer Protocol is a standard network protocol used for the transfer of computer files between a client and server on a computer network.

3.5 TLS

Transport Layer Security is a cryptographic protocol designed to provide communications security over a computer network

3.6 WPA2

Wi-Fi Protected Access II (WPA2) is a security protocol developed by the Wi-Fi Alliance to secure wireless computer networks.

3.7 Cryptography

A discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorized use.

3.8 Protocol

Formatting rules that specify how data is packaged into messages send and received.

4. Responsibility

4.1 Management

Management is responsible for classifying information access levels, also to ensure users and managers handling sensitive information are aware of any penalties for misuse of information.

4.2 Director

Director is responsible to adhere to the Public Service Orders

4.3 Network Administrators (NA)

Network Administrators are responsible to maintain network security to help protect against malware intrusions. NA is also responsible to ensure users have the right access to sensitive information and to monitor and protect the network from malware intrusions.

5. Content

5.1 Information Transfer

When dealing with information, staff shall follow the rules stated in the "ISMS03_0006_Information Classification and Handling Guideline."

5.1.1 Paper-based information not needed must be disposed of by shredding.

5.1.2 Staff (e.g. secretaries as they deal with incoming/outgoing correspondence) are reminded to not discuss and divulge any of the information that they come across.

5.1.3 Facsimile shall be accessed by authorized personnel only.

5.1.4 Public officers are governed by the PSO.

5.1.5 Suppliers Agreement

Any supplier that signs a contract with DOT shall abide by the non-disclosure agreement stipulated and shall abide by laws and regulations identified in the procedure" ISMS03_0022_Information Security-Related Laws and Regulations."

5.2 Transmission Channel

5.2.1 All confidential or restricted information transmitted through email to an email address outside of DOT's mandate must be encrypted. The transfer of such information outside of DOT's domain must be authorized by the Director or senior officer. The authorization must be issued in advance of the first instance and will apply thereafter if necessary.

5.2.2 Where confidential and restricted information is transmitted through a public network (for example the internet) to an external third party, information must be

encrypted first or sent via a secure channel (for example: Secure FTP, TLS, VPN, etc…). The transfer must be authorized by the Director of DOT. The authorization must be issued in advance of the first instance and will apply thereafter if necessary.

5.2.3 All confidential and restricted information transmitted around existing and new installations of wireless networks must be encrypted using WPA 2 (Wi-Fi Protected Access) or better.

5.2.4 Use of cryptographic techniques to protect the confidentiality, integrity and authenticity of information.

5.2.5 The Network Administrators shall take appropriate precautions so as not to reveal confidential information about the network's infrastructure.

5.2.6 All data about the network is kept within DOT. Information about the network is not forwarded to any personal external email address.

5.2.7 Joint effort is needed between the Network Administrators and Management to protect information from interception, copying, modification, misrouting and destruction.

5.2.8 Network Administrators are responsible for ensuring all unused ports are locked, monitoring network traffic, logs and any capturing tools for trends and possible attacks.

5.2.9 Network Administrators are responsible for ensuring that user access rights are properly configured and reviewed to avoid unauthorized access to information.

5.2.10 Data that management classifies to be sensitive (confidential or restricted) are protected by regular access rights.

5.2.11 Management is responsible for classifying the information, so the Network Administrators can properly configure the access rights on data and files.

5.2.12 All noncompliance (of the policy) is addressed at the management's level.

5.2.13 Management ensures that users with access to sensitive (confidential or restricted) data are aware of any penalties for deliberate information leakage or misuse, see "Public Service Orders."

6. Reference

Public Service Orders

ISMS03_0006_Information Classification and Handling Guideline

ISMS03_0022_Information Security-Related Laws and Regulations

7. Form

None