Office of the Chief Information Officer Directive: IT 9.06	Published: 04/2019
Chapter: Data Security	Last Review: 01/2022
Subject: **Data Encryption**	

1 DIRECTIVE

1.01 Data encryption tools must be available as needed to ensure protection of sensitive data. These tools must be considered under any of the following circumstances:

(a) Data resides on a shared-use or non-secure computer;

(b) Data is transmitted through a hostile environment. Portable media containing sensitive data that are physically transported outside the enterprise include, but are not limited to, laptops, tablets, smartphones, USB keys, external hard drives and CDs/DVDs. Data in transit on the Internet or other unprotected networks and needing protection may include email, email attachments, backup data for offsite storage, data provided from a company's website, and data or messages transmitted using FTP or instant messaging programs;

(c) Sensitive data requires protection from unauthorized use or disclosure;

(d) Sensitive messages must be protected against either disclosure or spoofing (impersonating) the original sender.

2 PURPOSE

2.01 The purpose of Directive is to ensure that sensitive data can be proactively protected to ensure:

- Confidentiality – protecting data from unauthorized access or disclosure
- Integrity – ensuring data is not changed in transit
- Accountability – authenticating data origin, so senders cannot deny sending it

3 SCOPE

3.01 This Directive applies to;

(a) IT Technical Support personnel who investigate software to be implemented;

(b) IT Operations personnel who prepare scripts for system backup, either to portable media or for transfer across a hostile network;

(c) IT systems end users who carry sensitive data offsite on portable media or transmit sensitive data across a hostile network.

4 RESPONSIBILITY

4.01 IT Technical Support is responsible for:

(a) Periodically evaluating encryption requirements for sensitive data;

(b) Providing software and hardware tools and processes (for example, key generation and management processes) to facilitate encryption;

(c) Providing IT Operations and end users with the training needed to evaluate what data may need encryption and to use the tools provided by the organization to encrypt their data effectively.

4.02 IT Operations staff are responsible for:

(a) Identifying sensitive data that they store or prepare for transmission through a hostile environment;

(b) Implementing tools provided to protect the data while in transit;

(c) Managing encryption keys enabling decryption of all encrypted data under their control.

4.03 IT systems end users are responsible for:

(a) Identifying sensitive data that they manage on shared-use computers or computers in an insecure environment;

(b) Identifying sensitive data that they load onto portable media for transport or processing offsite;

(c) Identifying sensitive data that they transmit on unsecure networks, for example emails and email attachments;

(d) Encrypting all sensitive data for each of above cases, using tools provided by the organization;

(e) Managing encryption keys according to the organization's protocols;

(f) Securely communicating the decryption keys to approved recipients of encrypted data;

(g) Reporting issues or challenges with implementing or applying encryption tools to IT Technical Support so that corrective action can be taken;

(h) Following all other policies and procedures implemented regarding encryption practices.

5 DEFINITIONS

5.01 "**Decryption of data**" is the process of undoing the transformation of encrypted data so it may be read normally. (See "**Encryption of data**" below).

5.02 "**Encryption of data**" is the transformation of data by applying a formula or algorithm and storing or transmitting it in its transformed state so that it is not

readable unless the reader knows how to undo the transformation (that is, decrypt the data).

5.03 **"Business Owner"** is a senior member within the organization who is accountable for overall management of defined data set for a line of business. The data business owner has decision-making authority for who accesses and uses the data, and is usually supported by data stewards. They approve processes and policies to uphold data quality and standardize data management processes.

5.04 "**Hostile environment**" refers to any environment that can imperil data security or integrity (perils include theft and unauthorized access or alteration).

5.05 "**Keys**" refer to anything used with the encryption algorithm to encrypt and decrypt information. A key can be a password or passphrase, or hardware devices or software known as "tokens". For stronger encryption, multiple keys, for example a password and a token may be employed.

5.06 "**Token**" See "**Keys**" above.

5.07 **"Sensitive Data"** is data that requires a high degree of confidentiality – It is "sensitive" to unauthorized disclosure or loss.

The desired degree of secrecy about such data is known as its sensitivity. Sensitivity is based upon a calculation of the damage to reputation or financial loss that the release of the data would cause.

6 RELATED DIRECTIVES

OCIO IT 5.06 – Records Retention
OCIO IT 9.03 – Data Access Controls
OCIO IT 9.05 – Data Disposal
OCIO IT 10.03 – Remote Access
OCIO IT 10.04 – Wireless Network
OCIO IT 10.06 – File Transfer Protocol (FTP)
OCIO IT 10.07 – Email Security
OCIO IT 10.08 – Instant Messaging
OCIO IT 10.09 – Electronic Commerce
OCIO IT 11.06 – Backup Data Stored Offsite
OCIO IT 13.07 – Removable Media
OCIO IT 13.08 – Portable Computers