Office of the Chief Information Officer Directive: IT 9.05	Published: 04/2019
Chapter: Data Security	Last Review: 01/2022
Subject: **Data Disposal**	

1 DIRECTIVE

1.01 Data must be disposed using appropriate procedures corresponding to the classification of the data at the time of disposal.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that classified data is disposed of securely in a manner that maintains confidentiality of the information.

3 SCOPE

3.01 This directive applies to all employees who own or control data.

4 RESPONSIBILITY

4.01 Business owners must review the data's classification at time of disposal. This will ensure that necessary procedures are executed for the data's disposal without invoking the extra expense of disposing of data that was classified at a high level during its lifetime and may be disposed of less expensively if its classification may be downgraded.

4.02 Operations staff must follow the procedures defined for data corresponding to its classification at time of disposal.

4.03 Department heads are responsible for:

(a) Ensuring adherence to this policy within their teams;

(b) Identifying data that requires disposal, and working with users and the Information Technology Service Delivery Organization (IT SDO) for data disposal needs;

(c) Reviewing, completing or authorizing documentation and providing information required under this policy; and

(d) Ensuring that disposals by IT and users in their teams are commensurate with the applicable data classification and data impact levels.

4.04 Business owners are responsible for determining data classification, access privileges and disposal or retention rules governing the data they own.

4.05 Users are responsible for ensuring or contributing to the secure disposal of their data.

4.06 The Information Technology Service Delivery Organization (IT SDO) is

responsible for providing its expertise when required to:

(a) Assist department heads and users with disposal requests;

(b) Obtain approvals and communicate appropriately regarding data disposal;

(c) Determine the best method to dispose of data;

(d) Perform all of the required sanitization steps;

(f) Verify the success of sanitization; and

(g) Complete any documents and information-sharing required.

4.07 Others in the organization, for instance, legal counsel/privacy officers/risk managers, are responsible for performing their roles with respect to data disposal. This includes ensuring the backup and retention of data is in accordance with records retention, privacy and other laws before data or hardware is disposed of or hardware is redeployed.

5 DEFINITIONS

5.01 "**Data classification**" is a data grouping scheme that identifies the sensitivity of data to improper disclosure. All data within a specified group have the same level of sensitivity and must be handled in the same way.

5.02 "**Data disposal**" refers to destroying obsolete data either by overwriting it on reusable media or physically destroying and trashing the media containing the obsolete data.

5.03 "**Data business owner**" 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.

6 RELATED DIRECTIVES

OCIO IT 9.01 – Data business ownership

OCIO IT 9.02 – Data Classification

OCIO IT 9.03 – Data Access Controls

OCIO IT 9.04 – Application Security Controls