

Storage of Business Information Assets Standard

OSP Document Number IM28-02	Table of Contents 1 Purpose 1 2 Scope 1 3 Definitions 1 4 Standard/Practice..... 2 5 Responsibilities..... 2 6 Related Policies 2 7 Related Operating Standards 2 8 History 2
Authorizing Unit University Legal Services Information Technologies	
Approval Authority General Counsel Chief Information Officer	
Implementation Authority Chief Information Officer	
Effective Date October 1, 2017	
Last Revision March 6, 2018	

- 1 Purpose** The purpose of this operating standard is to establish a standard for storing Business Information Assets.
- 2 Scope** This operating standard applies to Business Information Assets.
- 3 Definitions** In this operating standard:
- a) “Business Information Assets” mean Information Assets that relate to the University’s administrative functions, including its services, operations, finances, transactions, facilities, and student records.
 - b) “Control” means the responsibility for managing the access, handling, use and disposition of Information Assets.
 - c) “Custody” means the responsibility for storing Information Assets.
 - d) “Information Assets” mean information in the Custody or under the Control of the University, in any format or media, which relates to University’s administrative functions, including its services, operations, finances, transactions, facilities, and student records, or to teaching, scholarly, research or clinical activities.
 - e) “Managed Device” is a user device that is centrally managed and administered by the Information Technologies (IT) department over the network to ensure that it follows the configuration standards required to maintain security, reliability and accessibility of

Information Assets. This includes virus protection, software updates, and the ability for IT to keep both those up to date remotely.

f) "User" means any person who has authorized access to Information Assets.

- 4 Standard/Practice**
 - 4.1** Users shall store electronic Business Information Assets in Managed Devices.
 - 4.2** If Users download Business Information Assets to a laptop computer or portable device, the device has to be encrypted. Users are prohibited from disabling the encryption software at any time for any reason.
 - 4.3** Users shall store Business Information Assets in non-digital formats in facilities designated by University Archives, and in accordance with Information Management procedures established by University Archives.

- 5 Responsibilities**
 - 5.1** Information Technologies is responsible for:
 - a) Installing any software that is required to protect the University and Managed Devices.
 - b) Updating software, managing and scanning the device for viruses, and rebooting Managed Devices on a weekly basis.

- 6 Related Policies** [Information Asset Management Policy](#)

- 7 Related Operating Standards** [Information Security Classification Standard](#)

- 8 History**
 - September 14, 2017 Approved.
 - October 1, 2017 Effective.
 - March 6, 2018 Revised.
 - January 1, 2020 Editorial Revision. Updated format and links.