Storage Standards By Data Classification Level

	Approved or Recommended Storage Locations						Higher Risk or Prohibited Storage Locations				
	CCSU Hosted Services		CCSU Approved Cloud Services				CCSU Devices			Personal Device or Account (no formal agreement with CCSU)	
Data Type	Enterprise Systems & Secure Netshares [1]	Netshares (M:\, S:\, U:\, V:\)	Exchange Server and Hosted Exchange		OneDrive for Business (Office 365)	Hosted Services with Properly Reviewed and Executed Contracts [2]	University Owned and Supported Workstations & Laptops	University Owned Smart Phones & Tablets [3]	Multi-function Devices (printers, faxes, scanners) [4]	Personally owned device (home computer, smartphone, tablet, laptop, portable [USB thumb] drives) [5]	Personally maintained services (Dropbox, OneDrive, Gmail, Google Drive) [5]
			Sent or Shared Internally	Sent or Shared Externally							
DCL 3 (SSN, Bank account or debit card information, Credit Card # and cardholder information, Student Loan Data, GLBA, HIPAA)	Yes	No	No	No	No	Yes	No	No	No	No	No
DCL 2 (FERPA, Birth Date, Mother's maiden name, Academic Records, Student Records, Employee Records)	Yes	Yes	Yes [6]	No [7]	Yes	Yes	No	No	No	No	No
DCL 1 (Internal Memos, Minutes of Meetings, Internal Project Reports)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
DCL 0 (Advertising, Public Directory Information, Press Releases, Job Postings, Campus Maps)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No

[1] Examples of Enterprise Systems include Banner, ImageNow and CORE OneStep.

[2] Examples of Hosted Services include Adirondack and Medicat.

[3] Mobile/Portable devices must be passcode/pin protected and reported to University Police when missing.

[4] MFP hard drives must be removed and destroyed when decommissioned.

[5] Storing University business records within personally owned or maintained storage services exposes the institution to additional risk with respect to e-discovery, security breaches, and data retention and recovery. Furthermore, the University exerts a claim of ownership over business records saved on personally maintained devices or sites. Personally owned devices may access University data and systems remotely.

[6] FERPA correspondence with students is limited to my.ccsu.edu accounts.

[7] Sharing is limited to properly contracted partners and should be encrypted.

Reviewed at BCT and ITC

10/1/2019