University of Baltimore

Data Use Standards

Last Reviewed: 11/16/2020

Purpose
These Data Use Standards have been developed by the University of Baltimore as part of its Policy on Data Classification as required by the University System of Maryland Security Standards, as well as State and Federal laws and regulations. The purpose of this document is to outline requirements for the handling and protection of institutional data, whether it be public, proprietary, confidential or restricted.

Overview
Any member of the University of Baltimore community (staff, faculty, students, contractors, consultants, visitors, etc.) who creates, accesses, stores, processes, shares and/or destroys institutional data is responsible and accountable for complying with these standards. For this reason, all members of the university community should be able to identify the data classification of the information resources they work with in their university role in order to ensure that appropriate protections are met.

Standards
The table below defines the required safeguards for protecting data and data collections based on their classification. In addition to the standards specified in the table below, any data covered by federal and state laws; federal and state regulations; or other contractual agreements must meet the security requirements defined by those laws, regulations, or contracts (The University of Baltimore Policy on Data Classification classifies this data as “Category 4: Restricted”).

Table 1. Requirements for Security Controls Based on Data Classification

Security Control Category	Data Classification		
	Category 1 (Public)	***Category 2 (Proprietary)***	***Category 3 (Confidential)***
Granting Access or Sharing	• Viewing data is unrestricted • Modification of data is restricted to authorized individuals as needed for business-related roles	• Viewing and modification of data is restricted to authorized individuals as needed for business-related roles	• Viewing and modification of data is restricted to authorized individuals as needed for business-related roles

Security Control Category	Data Classification		
	Category 1 (Public)	***Category 2 (Proprietary)***	***Category 3 (Confidential)***
		• Authentication (preferably, based on NetID) required to access the data • Authorization to access is granted based on a documented request from the data steward	• Authentication (preferably, based on NetID) required to access the data • Authorization to access is granted based on a documented request from the data steward • The individual accessing the data must have a signed Non-Disclosure Agreement on record
Copying/Printing (applies to both paper and electronic forms)	• No restrictions	• Data should only be printed when there is a legitimate need (e.g. hard copy of the document required for compliance; document needs to be signed in person) • Copies must be limited to individuals with a need to know • Data should not be left unattended on a printer • The retention of paper copies must follow University retention policies	• Data should only be printed when there is a legitimate need (e.g. hard copy of the document required for compliance; document needs to be signed in person) • Copies must be limited to individuals authorized to access the data and who have signed an Non-Disclosure Agreement on record • Data should not be left unattended on a printer • Paper format documents must be stored in a secure

Security Control Category	Data Classification		
	Category 1 (Public)	***Category 2 (Proprietary)***	***Category 3 (Confidential)***
			location (e.g. locked office or cabinet) • The retention of paper copies must follow University retention policies
Remote Access to Systems Hosting the Data	• Access restricted to local network or virtual private network (VPN) service managed by the University of Baltimore	• Access restricted to local network or virtual private network (VPN) service managed by the University of Baltimore • Remote access by third party for technical support limited to authenticated, temporary access via the University of Baltimore Virtual Private Network (VPN) service	• Access restricted to local network or virtual private network (VPN) service managed by the University of Baltimore • Unsupervised remote access by third party for technical support not allowed
Data Storage	• Storage on a secure server recommended • Storage in a secure data center recommended	• Storage on a secure server recommended • Storage in a secure data center recommended • Should not be stored on a mobile device (e.g. cell phones, tablets, PDAs). If stored on a mobile device, data must be encrypted. • Should not be stored on portable electronic storage	• Storage on a secure server required • Storage in a secure data center required • Should not be stored on an individual workstation (e.g. desktop, laptop). If stored on individual workstation, data must be encrypted.

Security Control Category	Data Classification		
	Category 1 (Public)	***Category 2 (Proprietary)***	***Category 3 (Confidential)***
		media (e.g. CD/DVD ROMs, USB devices) unless encrypted • Must not be stored on the personally owned workstations and devices. • Must not be stored in cloud-based file hosting platforms (e.g. DropBox, OneDrive)	• Must not be stored on a mobile device (e.g. cell phones, tablets, PDAs) • Must not be stored on the personally owned workstations and devices. • Must not be stored on portable electronic storage media (e.g. CD/DVD ROMs, USB devices) unless encrypted and explicitly approved by OTS • Must not be stored in cloud-based file hosting platforms (e.g. DropBox, OneDrive)
Data Transmission	• No restrictions	• Encryption recommended (for example, via SSL/TLS, or secure file transfer protocols such as SFTP or FTPS)	• Encryption required (for example, via SSL/TLS, or secure file transfer protocols such as SFTP or FTPS • Cannot be transmitted via e-mail unless encrypted using OTS-approved encryption method

Security Control Category	Data Classification		
	Category 1 (Public)	***Category 2 (Proprietary)***	***Category 3 (Confidential)***
Exchanging Data with Third Party (e.g. Service Providers, Cloud Services)	• No restrictions	• Cloud Service Providers must complete Cloud Service Assessment (provided by OTS)	• Cloud Service Providers must complete Cloud Service Assessment (provided by OTS)
Backup/Disaster Recovery	• Backups required; daily backups recommended	• Daily backups required • Off-site storage is recommended	• Daily backups required • Off-site storage in a secure location required
Media Sanitization and Disposal	• All electronic storage media and equipment that is owned or leased by the University of Baltimore must comply with UB's media and equipment disposal and reuse procedures. All questions should be directed to the Office of Technology Services. (Equipment includes, but is not limited to: workstations, servers, laptops, cellphones, tablets and multi-function printers/copiers)	• All electronic storage media and equipment that is owned or leased by the University of Baltimore must comply with UB's media and equipment disposal and reuse procedures. All questions should be directed to the Office of Technology Services. (Equipment includes, but is not limited to: workstations, servers, laptops, cellphones, tablets and multi-function printers/copiers)	• All electronic storage media and equipment that is owned or leased by the University of Baltimore must comply with UB's media and equipment disposal and reuse procedures. All questions should be directed to the Office of Technology Services. (Equipment includes, but is not limited to: workstations, servers, laptops, cellphones, tablets and multi-function printers/copiers)

Security Control Category	Data Classification		
	Category 1 (Public)	***Category 2 (Proprietary)***	***Category 3 (Confidential)***
Training	• General security awareness training recommended • For system administrators – administrator specific training is recommended	• General security awareness training required • For system administrators - administrator specific training is recommended	• General security awareness training required • For system administrators – administrator specific training may be required • Applicable policy and regulation training is required