The Universities
AT SHADY GROVE

Data Retention Policy
USG Policy 6 (2.30) | Approved by the Executive Director, May 2019

I. Purpose and Applicability

The purpose of this policy is to specify guidelines in which identifies when data is no longer of value or use to USG, the process of retention, and when and how data should be purged.

The scope of this policy covers all USG data stored on USG-owned, USG-leased, and otherwise USG-provided systems and media, regardless of location.
Note that the need to retain certain information may be mandated by local, industry, or federal regulations and applicable laws. Where this policy differs from applicable regulations, the policy specified in the regulations will apply.

The Universities at Shady Grove is hereinafter referred to as "USG" and the Office of Information Technology as “OIT.” This policy will be reviewed annually to ensure continual compliance with USM IT Security Standards and other pertinent policies, laws and industry standards.

II. Definitions

A. *Backup***:** to copy data to a second location, solely for the purpose of safe keeping of that data.

B. *Data Retention*: to keep or retain a piece or set of data for a specific purpose or reason in relation to an organization’s business needs.

C. *Data Destruction:* to permanently destroy a piece or set of data

D. *Encryption*: the process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored**.**

E. *Encryption Key:* an alphanumeric series of characters that enables data to be encrypted and decrypted.

F. *Working Data Set*: any set of data elements which have not been achieved and have the potential to be used by the campus regularly for continual campus operations. This specifically excludes backup or archived data sets.

III. Reasons for Data Retention

A. USG does not wish to simply adopt a "save everything" mentality. That is not practical or cost-effective and would place an excessive burden on the organization to manage the constantly-growing amount of data. Some data, however, must be retained in order to protect USG's interests, preserve evidence, and generally conform to good business practices.

IV. Data Duplication

A. As data storage increases in size and decreases in cost, companies often err on the side of storing data in several places on the network. A common example of this is where a single file may be stored on a local user's machine, on a central file server, and again on a backup system. When identifying and classifying USG's data, it is important to also understand where that data may be stored, particularly as duplicate copies, so that this policy may be applied to all duplicates of the information. For example, data copied to USB flash drives or printed out is considered a copy under this policy and must adhere to the retention schedule in this policy (See Appendix A).

B. All work data sets must adhere to the retention schedule in the policy (See Appendix A). Data may be further retained in archives or backups based on USG Backup Policy.

V. Retention Requirements

A. This section sets general guidelines and requirements for retaining the different types of data sets stored and utilized by USG. USG may be required to retain data sets for longer or shorter periods as required by others policies, laws and regulations, legal action, intellectual property, or incident and other internal investigations. Please refer to Appendix A of this policy for the official retention schedule for each type of data or data set.

B. If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

VI. Data Destruction

A. Data destruction is a critical component of a data retention policy. Data destruction ensures that large amounts of data do not overburden USG’s IT resources, which make data management and data retrieval increasingly complex and expensive, and protects the campus from litigation or consequences due to violation of other polices and regulations. In conjunction with this policy data must be destroyed is accordance with the USG Data Classification Policy 6 (2.10), as well as, comply with this policy’s data retention schedule (see Appendix A).

B. Data destruction exemptions maybe granted under normal circumstances by the Director of OIT. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor to be considered for an exemption.

C. USG specifically directs users not to destroy data in violation of this policy. Particularly forbidden is destroying data that a user may feel is harmful to himself or herself, or destroying data in an attempt to cover up a violation of law or USG policy. Destruction of data is not permitted when the data or data set is involved in the following:

1. Litigation (criminal or civil)

2. Accident investigation
3. Security incident investigation
4. Violation of regulatory requirements

VII. Enforcement

A. The enforcement of this policy will be carried out by authorized USG OIT personnel designated by the Director of OIT and USG Senior Leadership. Violations may result in disciplinary actions, which may include suspension, restriction, or revocation of access. Where illegal activities or theft of USG property (physical or intellectual) are suspected, USG may report such activities to the state/federal law enforcement authorities.

VIII. Revision History

Date	Description	Revised By
06/15/2018	Initial Policy Creation	Russell Schlosburg

IX. Related Documents

A. USM IT Security Standards v4
http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf

Appendix A: Retention Schedule

General

Type of Data	Retention Period	Special Instructions
Personal	May be destroyed when no longer needed	
Public	May be destroyed when no longer needed	

Clearinghouse Data

Type of Data	Retention Period	Special Instructions
Emergency/Safety and Security	**3 years;** from when each record has expired and has been deactivated.*	
Operational/Service	**3 years;** from when each record has expired and has been deactivated.*	
Assessment/Research	All data is received and owned by USM. Data retention is based on applicable USM policies.	

* - if an expiration date does not exist use the last modified date followed by the created date if last modified is not available.