The Universities
AT SHADY GROVE

Backup Policy
USG Policy 6 (3.00) | Approved by the Executive Director, May 2019

I. Purpose and Applicability

The purpose of this policy is to provide a consistent framework to apply to the backup process. The policy will provide specific information to ensure backups are available and useful when needed.

This policy applies to all data stored on USG systems, including third-party and cloud solutions. The policy covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures.

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. *Backup Media*: any storage devices that are used to maintain data for backup purposes. These are often magnetic tapes, CDs, DVDs, or hard drives.

C. *Full Backup*: backup that makes a complete copy of the target data.

D. *Incremental Backup*: a backup that only backs up files that have changed in a designated time period, typically since the last backup was run.

E. *Restoration*: also called "recovery." The process of restoring the data from its backup-up state to its normal state so that it can be used and accessed in a regular manner.

III. Data to be Backed Up

A. A backup policy must balance the importance of the data to be backed up with the burden such backups place on the users, network resources, and the backup administrator. Data to be backed up will include all data determined to be essential to USG operation, instructional delivery, and/or employee job function based on USG Business Continuity Plan.

B. It is the user's responsibility to ensure any data of importance is stored on a USG OIT approved medium and actively backed up for appropriate preservation and recovery.

IV. Backup Data Identification

A. USG must identify what data is most critical to its organization. The following guidelines should be used to classify data for backup in addition to the USG Data Classification Policy 6 (2.10):

1. Data loss impact to students and faculty.
2. Data loss impact to USG and/or Partner staff.
3. Risk to human health / environment.
4. Negative / limited impact to students, faculty and staff satisfaction.’
5. Direct or indirect damage to USG’s Mission Statement.
6. Class / Coursework / Lab productivity degradation
7. Employee productivity degradation.
8. Departmental / Services degradation.

V. Backup Frequency

A. Backup frequency is critical to successful data recovery. USG will implement a backup schedule which will allow for sufficient data recovery in the event of an incident, while avoiding an undue burden on the users, network, and backup administrator. The backup schedule will take into account the impact of loss and risk to USG’s business continuity.

VI. Off-Site Storage

A. Geographic separation from the backups must be maintained, to some degree, in order to protect from fire, flood, or other regional or large-scale catastrophes. Offsite storage must be balanced with the time required to recover the data, which must meet USG's uptime requirements. USG recommends that all data stored on premise should be backed up to an USG approved off-site storage location insuring that appropriate security measures, at rest and in transit, are maintained based on USG’s Data Classification Policy 6 (2.10).

VII. On-Site Backup Storage

A. Storage of backups is a serious issue and one that requires careful consideration. Since backups contain critical, and often confidential, company data, precautions must be taken that are commensurate to the type of data being stored. USG has set the following guidelines for backup storage.

B. When stored onsite, backups should be kept in physically access-controlled area on devices that require authentication. If authentication is not possible or technically feasible other compensating controls may be applied.

VIII. Backup Retention

A. When determining the frequency and time required for backup retention, USG must determine what number of stored copies of backup-up data is sufficient to effectively mitigate risk while preserving required data. USG recommends that backups be maintained for a minimum of 14 calendar days and no longer than 6 months.

IX. Restoration Procedures & Documentation

A. The data restoration procedures must be tested and documented. Documentation should include exactly who is responsible for the restore, how it is performed, under what circumstances it is to be performed, and how long it should take from request to restoration. It is extremely important that the procedures are clear and concise such that they are not misinterpreted by readers other than the backup administrator and/or confusing during a time of crisis.

X. 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.

XI. Revision History

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

XII. Related Documents

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