Backup Policy
TEC 17.0
Information Technology

Policy Type: Operational
Applies to: Office of Information Technology
Related Policies: IT DR Plan, Information Security Plan

POLICY DATES

Issued: May 2023
Revised: May 2023
Edited: May 2023
Reviewed: May 2023

The purpose of this policy is to provide standards for the continuity, restoration, and recovery of data in the event of an equipment failure, intentional destruction of data or natural disaster.
All university data residing on systems maintained by the Office of Information Technology in the Network Operations Center (NOC) must be backed up for the purpose of recovery on a regular basis. This policy outlines the minimum requirements for the creation and retention of backups.

This policy applies to all university data residing on systems maintained in the Network Operations Center. IT is responsible for the backup of data stored in the NOC. The backup of data stored on individual workstations, whether they are university or personally owned, is the responsibility of the user. Users should consult with the IT helpdesk for local backup procedures.

The University does partner with many vendors who support systems in the cloud as Software as a Service (SaaS). Those vendors in partnership with Mount Union backup and support those particular systems. This policy does not apply to them.

Definitions

Term	Definition
Backup	Backup is saving or copying information onto digital storage media (which includes cloud storage)
Full Backup	A copy of every file.
Partial Backup	A copy of selected files.
Network Operations Center (NOC)	On premise data center, where servers are located. This location is secure. All institutional on-premises servers must be located here.
Incremental Backup	A copy of files that have changed (i.e., modified or created) since the last backup performed.
Differential Backup	A copy of files that have changed (i.e., modified or created) since a specific data and time.
Off Site Backup location	IT uses Wasabi for cloud backup storage location
Backup software	IT uses Veeam for backups software/solution.
IT Resources	IT resources may include computing, networking, communications, application, and telecommunication systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, software as a service (SaaS) vendor, and related materials and services
Restore	Restore is to return data that has been lost, stolen or damaged to its original condition or to move data to a new location.

The University requires computer systems maintained by the Office of Information Technology on premise within the network operations center be backed up on a regular basis, that the backup be stored at a secure off-site location, and that recovery tests are performed on a regular basis. As a result, IT will adhere to information technology best practices which call for daily, weekly, and monthly system backups. This scheme allows systems to be restored with at most one working days' data missing.

The purpose of the system backup is to provide a means to restore the integrity of the computer systems in the event of a hardware, software failure or physical disaster or provide a measure of protection against human error or the inadvertent deletion of important files. System backups are not intended to serve as an archival copy or to meet records retention requirements.

The office of Information Technology has an on-premises backup server and uses Veeam software for backup and recovery purposes. IT is also using Wasabi for cloud backup solution. Wasabi combined with Veeam backup offers data protection.

Technical/Network Services within the Office of Information Technology are responsible to perform, schedule, support, log and document backup and recovery procedures. This includes the testing of restoring of data. Full backups are performed every Sunday, then incremental for the remainder of the week. This is for all systems within data center/NOC.

Frequency of system/application/network file backups:
Incremental backups will be performed daily. Full backups are performed every Saturday. Incremental backups will be saved for seven days on premise to backup server and synchronized to the cloud. Thirty days of incremental are stored in the cloud with Wasabi. A full system backup will be performed weekly, each Saturday. The weekly is kept for four weeks in the cloud/Wasabi. Monthly are kept for six months. The first weekly backup of the month will be marked as a monthly backup.

Frequency of email backups:
The university uses Microsoft (Exchange Online) for Email. Emails will not be backed up. Items that are moved to the deleted items folder will be retained until that folder is cleared out. Once items are removed from the deleted items folder or permanently deleted, they can be recovered up to 30 days after removal. In cases of legal retention requirements, IT must be informed by Human Resources or the VP of Business Affairs or the university general counsel whose records must be retained so a legal hold can be placed on a faculty/staff/student mailbox, provided that mailbox still exists. Once a legal hold is placed on a mailbox all records are retained until the hold is lifted.

Frequency of desktop backups:
Backups of desktops, laptops, tables and VDI's are not supported by IT. It is the responsibility of the faculty/staff/student to backup their systems. We encourage people to save documents to their MS OneDrive. In the event of a legal retention, a laptop, desktop or tablet may be held for a period of time until that legal hold has been lifted.

Storage:
Daily incremental, weekly and monthly backups are stored to our onsite backup server and cloud storage location. Access to the secure off-site cloud location and the ability to request backups from this location is limited to the Director of IT for Security, CIO, Manager of Technical Services and the named technicians whose duties require them to perform system backups.

Recovery Testing:
IT Network technicians will perform quarterly recovery testing on select system and network backups to determine if the files and data can be restored.

Exceptions:
In the unlikely event that a system cannot conform to this policy, the appropriate director will inform the Office of Information Technology and specific actions will need to be taken to comply with backup policies.

Responsibilities

Position or Office	Responsibilities
Information Technology	(CIO, DIR of IT for Security, Mgr. of Tech Services)

Applies to: Office of Information Technology

Resources

Backup Procedures are located in the Information Technology Team -> Technical Services Private Channel ->Backups -> Veeam ->Backup Procedures.docx

Contacts

Subject	Office	Telephone	E-mail/URL
CIO, Dir. IT for Operations, Mgr. Tech services	Office of Human Resources	330-823-2854	IT@mountunion.edu

History

All changes must be listed sequentially, including edits and reviews. Note when the policy name or number changes.

Issued:	May 2023
Revised:	May 2023
Edited:	May 2023
Reviewed:	May 2023