Policy: **IT BACKUP POLICY**

Policy Title	**IT BACKUP POLICY**
Policy Ref:	2024_Backup_Po_V2
Effective Date	June 2024
Responsible Office	Provost Office
Responsible Executive(s)	IT Department

Desktop and Laptop Backup Policy

Local documents stored on desktop and laptop computers should be backed up so the documents and files can be restored in the event of a physical problem with the machine or if individual files or folders are inadvertently removed.

- University faculty and staff have access to a networked drive provided by Information Technology. Faculty and staff in AUM University may have access to division-specific resources.

- All network storage resources must have a backup policy. Non-IT domains need an IT-approved backup policy for Desktop and Laptop Computers. A current copy of this policy must be on file with IT Individuals using non-IT domains must follow the approved backup policy.

Backup Modes

- Network file storage is the main backup mode.
- Files may be copied to once-writeable media (CDs, DVDs) or rewriteable storage media (e.g., hard disks, other magnetic media, and flash memory devices/thumb drives in addition to the Main Data Storage). These media must be stored in a secure location.
- Cloud Backup Storage via Office365 OneDrive

Server Backup Policy

Backup procedures and policies are developed for two purposes, disaster recovery and file recovery. In the event of a catastrophe, due to a physical disaster, personnel error, or other misfortune, reliable backups must provide timely and

accurate restoration of all functions of the organization. Individual file recovery may be required to restore programs, information, And- or other data that has become corrupted or inadvertently removed.

- Backup procedures for all servers must be approved by IT. Procedures must include an appropriate time schedule, media description, storage, documentation, and testing process.
- Knowledge of the backup location and access to the site should be limited to a few key people within the organization, but at least two individuals should have access to the facility.

All AUM systems and networks are fully secured against any attack and violation. We have a firewall system on the premise that protects all AUM servers, AUM network, Computers and internet access. Besides all AUM sites and remote learning are fully secured. Also, all the servers and PCs have antivirus systems to protect them. In addition, we have Office 365 mail and office solution that is fully secured by Microsoft company which also provides One Drive where the students, Faculties and the Staff will be able to secure their files and documents on it and it gives the ability to share their documents in a very secured manner. In addition, all the AUM systems are secured with very restrictive access permissions where the access permissions is given as per the business needs after getting a proper approvals. All the personal information data for Students, Staff and Faculties are fully secured against anonymous access and no one can access it without a proper access permission. All the information data for the students will be placed on the student's information system, OIS, where no one can see the data of others and no one will have an access without a proper permission.