Backup and Restoration of University Owned Data	**6-011** **TECHNOLOGY SERVICES** **December 2019**

GENERAL STATEMENT

1.01 The purpose of this policy is to ensure server and data continuity and to support the retrieval and restoration of archived information in the event of a natural disaster, equipment failure, and/or accidental loss of files.

POLICY

2.01 Procedures shall be in place to create backup copies of all mission-critical data stored on OSU Institute of Technology (OSUIT) network servers.

2.02 Only mission-critical, university-owned data should be stored on the production network servers.

2.03 Procedures shall be in place to test the ability to restore backups.

2.04 Methods shall be implemented for authorized users to gain access to the backup data quickly.

2.05 These procedures shall be updated annually to accommodate changes in policies or procedures at OSUIT.

2.06 Off-site storage shall be used for critical backups and documentation. Access to the off-site storage shall be secure.

2.07 Backing up of data not stored on network servers shall be the responsibility of the user.

2.08 In the event university-owned data is stored on a cloud service, the unit purchasing the cloud service is responsible for assuring there is a service-level agreement in the contract with the cloud provider ensuring that they provide the same or greater level of backup availability as if the data was stored using on-site network servers.

PROCEDURES

3.01 Technology Services shall be responsible for backing up university-owned data stored on the network servers**.** Infrastructure Administrator (IA) shall have the responsibility of ensuring the completeness of the automated backup process each day, reporting any failures and taking appropriate action to correct any problems.

3.02 The IA shall check the event logs and backup reports daily. The IA shall restore random files from backup each Monday to confirm the backups are restorable.

3.03 An incremental backup of network server data shall be captured to disc daily with an automated backup send to a remote disaster recovery site.

3.04 Backup snapshots shall be available on disc of the last 28 days at a minimum. Beyond this time period, monthly snapshots shall be available.

3.05 In the event that a server data file needs to be restored, the user shall call or email the service desk with the request. The restoration of lost or damaged file(s) shall be completed within a 48-hour time frame.

3.06 Data which has not been accessed in the last year may be moved to a lower storage tier.

Approved: February 2013
Revised: July 2016
Revised: December 2019