The University of the South
Backup and Recovery Policy

Purpose

The purpose of this policy is to define the requirements for backup and recovery of information, software and systems of the University of the South which are maintained by the Strategic Digital Infrastructure department. The policy described within this document follows industry standards for providing disaster recovery capabilities for the University's computer systems based upon the business needs of the University. Backup copies of information, software and system images should be taken and tested regularly.

Scope

This policy applies to the systems maintained by the Strategic Digital Infrastructure (SDI) department in the Library and Information Technology Services (LITS) division.

Individual University-issued computers are not in the scope of this policy and are the responsibility of the user of the computer. Helpdesk personnel will assist as requested by providing recommendations and assistance in the implementation of individual backup procedures.

Responsible Party

The Associate Provost of the Library and Information Technology Services division of the University is responsible for maintaining this policy and may be contacted with any questions.

Definitions

Term	Definition
Hosted System	A system that is installed and managed by a software manufacturer or a third-party vendor in a remote data center. University staff do not serve as the system administrators for the system.
Infrastructure as a Service (IaaS)	Infrastructure as a service (IaaS) is a service provided by a vendor that typically includes hardware, storage, servers and data center space or network components. University staff are not responsible for the hardware but do serve as the system administrators for the system.
Information Technology (IT)	Information Technology is part of the Library and Information Technology Services division of the University. IT is charged with establishing, monitoring and maintaining

	information technology systems and services. IT includes both the Technology, Access and Support department and the Strategic Digital Infrastructure department.
LITS	Library and Information Technology Services is a division of the University that encompasses the library and information technology functions of the University.
On-premise Servers	On-premise servers are physically located on University property. University staff are responsible for the hardware maintenance of these systems and also serve as the system administrators for the systems.
RAID	Redundant Array of Independent Disks is a data storage virtualization technology which is used to improve the availability, performance, and reliability of disk drives. Depending on the configuration, one or more disk drives can fail without causing a loss of data.
SDI	Strategic Digital Infrastructure is a department within the Library and Information Technology Services division of the University.
SDI Procedures Manual	A collection of written procedures for key functions performed by the SDI staff. The procedures help ensure the continued functioning of the department during an employee's absence.

Policy Statement

The file and application servers of the University are installed in protected environments utilizing high-availability technology such as a redundant array of independent disks (RAID) to help ensure the availability of the University systems and to protect against the loss of data or applications due to hardware failure. This technology is highly reliable, but does not provide 100% assurance as a hardware failure is possible. The loss of data or applications can also occur from software failures.

Therefore, accurate and timely backups of the operating system, system and user files of the file and application servers of the University shall be conducted routinely. These backups are necessary to ensure timely and accurate recovery of the file and application servers in the event of hardware or software failures to minimize disruption to the University. Each server shall be evaluated to determine the schedules and retention for the backups dependent upon the significance, size, and frequency of data variation of information stored on the servers. Sufficient backups of the systems are to be made so that under all non-disaster circumstances no more than one day's worth of information will be lost due to a non-catastrophic system failure. Also, on critical systems, backups of databases and/or files are to be taken during processing runs in the event of a processing error.

Consequences

All University of the South employees are expected to abide by this policy. Violations of this policy will be treated like other allegations of wrongdoing at the University of the South. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for noncompliance may include, but are not limited to, one or more of the following:

- Disciplinary action according to applicable University policies;
- Termination of employment.

Responsibilities

The University utilizes three different types of hardware for housing servers and applications. These three types are hosted, on-premise, and infrastructure-as-a-service (IaaS). Due to the lack of access to hosted systems, it is the responsibility of the vendor or third-party to perform appropriate backups and/or restoration as needed. Contracts for hosted systems should clearly define this responsibility. SDI staff are responsible for performing backups of on-premise and IaaS servers.

Procedures

On-premise systems are backed up to a local backup disk service and backups of critical systems are replicated to a cloud-based repository. The servers housed in infrastructure-as-a-service (IaaS) will be backed up to a cloud-based repository. The on-premise backup storage is in a secure, temperature and electrical power controlled environment. The cloud-based backup repository is provided by a Veeam certified service provider that is ISO certified and is also a secure, temperature and electrical power controlled environment. Traffic between the servers and the cloud backup repository is encrypted to protect the data and the data stored in the cloud repository is encrypted. The encryption key is only known by SDI personnel and not the cloud repository personnel to ensure the privacy of the data.

Backup Procedures

Backup procedures are documented and included in the SDI procedures manual which is maintained by the Director of Strategic Digital Infrastructure. The majority of backup jobs are automated and the backup logs are e-mailed to the appropriate backup administrator. These logs are to be reviewed daily by the assigned backup administrator. Any failed jobs are to be investigated and any issues are to be corrected. Manual backup jobs will be run as necessary to replace failed jobs.

Recovery Procedures

Procedures for recovery of either single files or an entire system are documented and included in the SDI procedures manual which is maintained by the Director of Strategic Digital Infrastructure.

In the event of a full system failure that requires a system reload, the recovery procedures shall be utilized as documented in the procedures manual for IT staff.

Periodic tests of the recovery procedures should be conducted to ensure the reliability of the backup procedures and media. The restoration of an on-premise server from the local backup repository and a IaaS server from the cloud repository will be conducted once per year. These tests will be documented and kept by the Director of Strategic Digital Infrastructure.

Special Considerations

Databases are complex data structures which are constantly being updated and therefore cannot reliably be backed up with traditional backup software. The database management tools are used to back up the data to ordinary flat data files. The database management tools are also used to restore the flat data files to the database if needed. The ordinary data files are included in the disk and cloud backups and are used for any restoration.

REVISION DATE: August 24, 2021