ADMINISTRATIVE POLICY

Backup & Recovery

POLICY STATEMENT

Information & Technology Services is responsible for providing adequate backups to ensure the recovery of data and systems in the event of failure. These backup provisions will allow university business processes to be resumed in a reasonable amount of time with minimal loss of data. Since hardware and software failures can take many forms and may occur over time, institutional data backups should be maintained.

This policy does not refer to the backing up of data that resides on individual workstations or mobile devices. Responsibility for backing up of data on local systems rests with the individual user. It is strongly encouraged that end users save their data to network file servers so that the data is backed up in accordance with this policy.

REASON FOR POLICY

This policy defines the requirements for maintaining and recovering backup copies of critical Nevada State University data created, processed, or stored on Nevada State University servers managed by Information & Technology Services.

PROCEDURES

Schedule

Full Data Backups - All critical data resident on Nevada State University servers must be fully backed-up on a weekly basis at minimum.

Incremental Data Backups - All critical data resident on Nevada State University servers must be incrementally backed-up on a daily basis at minimum.

Off-Site Backups - All critical data resident on Nevada State University servers must be backed-up to an off-site location on a monthly basis at minimum.

Backup Procedures

On-Site Backup - At least one generation of backup files must be maintained in on-site data storage wherever production servers are located.

Off-Site Backups - At least one complete backup containing critical Nevada State University data must be stored off-site.

Workstation Backups - All critical data used on workstations should be placed on an institutional network file server or cloud storage to allow for backup. If, however, critical data

is stored on a local device, it is the data owner's responsibility to maintain a backup of that data.

Backup Security - All sensitive, valuable, or critical data recorded on backup computer media and stored outside Nevada State University offices must be encrypted.

Retention - At a minimum, backups should be retained for at least 30 days.

Testing and Review

Backup Recovery - Recovery procedures are to be tested on at least an annual basis.

Backup Review - Department managers or their delegates must ensure that proper backups of sensitive, critical, and valuable data are being made if such data is resident on personal computers, workstations, or other systems in their area. In addition, each location that is used to store Nevada State University backups must be reviewed at least annually to determine that the backup storage is functioning and secure.

CONTACTS

SUBJECT	CONTACT	PHONE	EMAIL
Primary Contact(s)	Brian Chongtai	702-992-2410	brian.chongtai@nevadastate.edu

DEFINITIONS

Backup: A copy of files or data made to facilitate recovery.

Critical Data: Data necessary for the day-to-day operations of the campus.

RELATED INFORMATION

HISTORY

Revised 8/5/24