Backup Policy for Chicago State University Systems

Policy Statement

Chicago State University (CSU) Information Technology Division (ITD) performs backups of all electronically stored information that is supported and managed by ITD for the purpose of restoring services in the event of failure resulting from a malfunction, corruption of data, failed hardware, or other conditions.

Purpose

The purpose of this policy is to define the backup/recovery policy for the information technology systems supported by ITD. This policy describes how CSU critical systems within and outside ITD must be protected to ensure services can be recovered and data is not lost in the event of a disaster.

Scope

This policy applies to all information technology systems at the University that have been identified as critical systems. Critical systems are systems that will be required to continue normal business operations of the University in the event of failure. It also applies to individual departments and users that store critical and sensitive data.

Definitions

1. Electronically stored information (ESI): General term for any electronic information stored on any medium (i.e., hard drive, back-up tapes, CDs, DVDs, flash drives, external drives, and any other form of electronic media capable of storing data) that can be retrieved and examined.
2. Archive: The saving of old or unused files on off-line mass storage media for the purpose of releasing on-line storage space.
3. Backup: The saving of electronic information on encrypted and protected mobile storage devices such as USB drive, disk, tape, or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
4. Disaster Recovery: The policies, process and procedures related to preparing for recovery of technology infrastructure critical to CSU operations after a natural or human induced event. Disaster recovery focuses on the restoring technology systems that support business functions that fail in the event of a disaster.
5. IT systems: The hardware and software used to store, retrieve, and manipulate information.
6. Restore: The process of bringing data back from off-line media and putting it on an online storage system when the data on the online storage system is lost or corrupt.

Responsibility

1. It is the responsibility of every campus community user to take reasonable care to protect and store confidential and sensitive data against physical theft or loss. It is ITD's responsibility to establish guidelines for the campus community users to perform backups and restoration of their data systems.
2. It is responsibility of each campus community user within its College, Department or Unit to identify any unique requirements for backup or restoration of data system and acquire encrypted, password protected storage medium (i.e., encrypted and password protected flash drives, USB

drives, CD, tapes, or other mechanism) that can be used to securely store its data and have the ability to restore data to its original state in the event of failure.

Policy

1. Each IT system will be backed up according to its unique characteristics and requirements.
2. Specific back up procedures for critical University systems are identified and shared with CSU's disaster recovery vendor, to allow for recovery of the University's services in the event of a disaster. Do we have to name the vendor?
3. ITD performs full and incremental backups of the University servers and applications that are managed by ITD.
4. Critical systems are backed up on daily basis and the data is transferred electronically to, CSU's disaster recovery partner.
5. ITD, on a semi-monthly basis rotates backup copies of IT system data off-site to US Bank safe deposit vault. NO Longer the case needs to remove. MO
6. It is recommended that the departments and users perform weekly full backups and daily incremental backups when storing sensitive and confidential University data. Storage of all data should be performed on encrypted, password protected equipment. Departments and users should avoid storing any critical, confidential, and sensitive information on their departmental servers or personal computers. ITD can assist in providing a secure location which is backed up as described above to store such University information.
7. The party responsible for making data backups will monthly, validate the efficacy of backup data and the ability to restore that data to its appropriate platform.
8. The switches and routers are backed up for the following reasons:
    a. Upgrade to networking equipment
    b. Changes to configuration
    c. Upgrades to any equipment that affects data flow (e.g.: spam filter, firewalls, etc.)
    d. Changes/upgrades to anything that affects the data link and network layer

   The configuration for the routers and switches are backed up to a tftp servers. After the files are stored on the tftp server, they are zipped, encrypted, and placed on a portable drive. The drive is sent to University's offsite storage.

Policy Exceptions and Maintenance

Waivers from certain and specific policy provisions may be sought following the CSU ITD approval Process. There are no exceptions to any provisions noted in this policy until and unless a waiver has been granted by ITD.

Enforcement

This Backup Policy supplements and compliments all other related information security policies, it does not supersede any such policy or vice versa. Where there are any perceived or unintended conflicts between CSU policies, they must be brought to the attention of ITD for immediate reconciliation.

Personnel found to have violated any provision of this policy may be subject to sanctions up to and including removal of access rights, termination of employment, termination of contract(s), and/or related civil or criminal penalties.

References

- NIST CSF: PR.IP-4

Version History

Version	Modified Date	Next Review	Approved Date	Approved By	Comments
1.0	11/3/2022	11/1/2023	11/6/2022	Donna Hart	