Collin College Technology Services (CC-TS)
Data Backup and Recovery - Information Security Procedure (ISP):

PURPOSE:

The purpose of the Data Backup and Recovery ISP is to manage and secure backup and restoration processes of critical data; prevent the loss of data in the case of administrator error or corruption of data, system failure, or disaster; and ensure periodic restoration of data to confirm it is recoverable in a useable form.

SCOPE:

The CC Data Backup and Recovery ISP applies to any data owner, data custodian, system administrator, and CC-TS staff that installs, operates, or maintains Collin College (CC) information technology resources.

STATEMENT:

1. CC-TS System Administrators are responsible for backing up CC-TS-managed servers and must implement a tested and auditable process to facilitate recovery from data loss.

2. All departments should store data on network storage (e.g., I and J drives) rather than local storage (e.g., PC or Mac hard drive). CC-TS does not back up local storage and will be the data owner's responsibility.

3. CC-TS System Administrators will perform daily data backups of all CC-TS managed servers containing critical data for the following purposes.

    - Individual drives and folders the data owner requests will be retained for 30 days.
    - CC will not be responsible for data stored on non-CC cloud storage systems (e.g., One Drive, Office 365 email), and data will be subject to vendor retention terms of service.

4. Determining which data and information are deemed 'critical' (e.g., confidential data and other data considered to be of institutional value) is the responsibility of the Data Owner. Data the Data Owner identifies as non-critical may be excluded from this ISP.

5. Alternative backup schedules and media management may be requested by the data owner commensurate with the criticality of the data and the capabilities of the tools used for data storage.

6. Records retention is the responsibility of the Data Owner. The CC-TS backups are not to be used to satisfy records retention and are not customized for all the varying retention periods.

7. Backup data for Production systems will be stored at a location that is physically different from the original data source.

8. Verification, through the restoration of backed-up data, must be performed regularly as defined by the CC-TS backup procedures document for the representative system.

9. Procedures for backing up critical data and the testing of the procedures must be documented. Such procedures must include, at a minimum, for each type of data:

    - A definition of the specific data to be backed up.
    - The backup method to be used (full backup, incremental backup, differential, mirror, or a combination).
    - The frequency and time of data backup.
    - The responsible party for data backup.
    - The storage sites for the backups.
    - The storage media to be used.
    - For data transferred during any backup process, end-to-end security of the transmission path must be ensured for confidential data.
    - The recovery process of backed-up data must be maintained, reviewed, and updated periodically to account for new technology, business changes, and migration of applications to alternative platforms.

PROCEDURE:

Backup:

1. Server backups are performed nightly by the backup system, Dell EMC IDPA, system, including holidays. The data is retained for 30 days.

2. The production system's data backups are stored at a location different from the Production system location. Backups are located at the Frisco campus, 15.5 miles from the Production data center.

3. Backups are performed and monitored by the backup team, System Administrators in Technology Services.

4. For non-DB type backups using IDPA, there are two backup types: initial and non-initial. In the case of non-initial backup, data changes (new bytes) since the last backup time are backed up.

5. DB-type backup is performed weekly with a full backup followed by several incremental.

6. Dell EMC IDPA stores all backups on disks. No tape media is used.

Recovery:

1. If data loss or data corruption occurs, the data owner opens a service request to the backup team in Technology Services. The ticket must provide full path names and the related time and dates for the data to be restored.

2. The backup team locates the appropriate backup and performs the restore.

3. The backup team notifies the data owner to verify the restore.

4. Upon approval from the data owner, the data restore ticket is closed.

Disaster Recovery Procedure:

1. In the event of a disaster, a service request is opened to the backup team in Technology Services.

2. If a hardware failure occurs, a ticket is opened to the vendor to receive a replacement. A field engineer from the vendor shall be on-site to perform the repair.

3. If there is data corruption on servers, follow the steps in the 'Recovery Procedure.'

4. If a physical-based server is corrupted, the system administrator team or Network administrator team (for Windows server only) rebuild the Operation system and restore the application data from the backup. Further database recovery is handed over to the DBA team if a database is involved. Further, Windows server recovery is handed over to the Application administrator team if the server is a Windows server.

5. The system administrator team performs a VM-level restore if a virtual machine-based server is corrupted. Further database recovery is handed over to the DBA team if a database is involved.

6. The Network administrator team handles network infrastructure and VMWare infrastructure recovery.

7. Upon approval from the server owner, the recovery ticket is closed.

Implementation Information

Review Frequency:	Annually
Responsible Person:	SVP – Campus Operations
Approved By:	Abe Johnson, Ed. D.
Approval Date:	02/09/2022

Revision History

Version:	Date:	Description:
1.0	02/09/2022	Initial document
1.1	10/28/2022	Annual Review – No Changes required.
1.2	11/08/2023	Annual Review – One Minor Change