Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Data Backup and Recovery Policy:

PURPOSE:
The purpose of the Data Backup Policy is to manage and secure backup and restoration processes and the media employed within these processes; 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 Clarendon College Data Backup policy applies to any data owner, data custodian, system administrator, and Clarendon College-IT staff that installs, operates, or maintains Clarendon College information technology resources. Appendix A of this policy shows a schematic diagram of the backup process.

POLICY STATEMENT:

1. Clarendon College-IT System Administrators are responsible for backing up Clarendon College-IT-managed servers and must implement a tested and auditable process to facilitate recovery from data loss.
2. All departments should store data on the network rather than local storage (e.g., PC or Mac hard drive). Clarendon College-IT does not back up local storage and will be the data owner's responsibility.
3. Clarendon College-IT will perform timely data backups of all Clarendon College-IT-managed servers containing critical data for the abovementioned purposes.
    a. Individual drives (redirected folders and mapped drives) and email will be retained for 90 days.
    b. All other data, such as Enterprise Application Data (e.g., CAMS Enterprise, Dynamics GP, and SQL data) and shared storage backups, will be retained for 30 days.
    c. Clarendon College will not be responsible for data stored on non-Clarendon College cloud storage systems (e.g., OneDrive), and data will be subject to that vendor's retention terms of service.
    d. Cloud retention of all data backups is 30 days.
    e. Learning Management System (LMS) backups are retained locally to the LMS for 30 days after the end of a term. They are then copied to the College's local server for retention for at least one year.
4. Determining which data and information is deemed 'critical' (e.g., confidential data and other data considered to be of institutional value) is the responsibility of the Data Owner under the Data Classification Policy. Data the Data Owner identifies as non-critical may be excluded from this policy.
    a. Alternative backup schedules and media management may be requested by the data owner commensurate with the criticality of the data and the

b. capabilities of the tools used for data storage.

5. Records retention is the responsibility of the Data Owner. The Clarendon College-IT backups are not to be used to satisfy the retention of records and are not customized for all the varying retention periods.
6. Monthly backup data will be stored in a location that is physically different from the original data source.
7. Verification must be performed regularly by restoring backed-up data as defined by the system's Clarendon College-IT backup procedures document.
8. Procedures for backing up critical data and testing the procedures must be documented. Such procedures must include, at a minimum, for each type of data:
    a. A definition of the specific data to be backed up.
    b. The backup method (full backup, incremental backup, differential, mirror, or a combination).
    c. The frequency and time of data backup.
    d. The number of generations of backed-up data to be maintained (both on-site and off-site).
    e. The responsible individual(s) for data backup.
    f. The storage site(s) for the backups.
    g. The storage media to be used.
    h. The naming convention for the labels on storage media.
        i. Any requirements concerning the data backup archives.
    i. The data transport modes.
    j. For data transferred during any backup process, end-to-end.
    k. K. Security of the transmission path must be ensured for confidential data.
    l. The recovery of backed-up data.
        i. Processes must be maintained, reviewed, and updated periodically to account for new technology, business changes, and migration of applications to alternative platforms.
    m. The destruction of obsolete backup media as described in Clarendon College Media Sanitization Policy.

9. Backup Schedule

The following table represents the approved critical data, backup schedule, and data retention:

Server/Host	Data Description	Recovery Points	Local Retention	Offsite Retention	Offsite Replication
Server1	Accounting Database (GP/SQL)	Hourly 24-hrs day	30 Rolling Days	3 Rolling Days	Update from 1 AM Nightly / SC Cloud to Hourly 24-hrs day
Server2	File shares	Hourly 24-hrs day	30 Rolling Days	3 Rolling Days	Update from 1 AM Nightly / SC Cloud to Hourly 24-hrs day
Server3	AD / Security	Hourly 24-hrs day	30 Rolling Days	3 Rolling Days	Update from 1 AM Nightly / SC Cloud to Hourly 24-hrs day
Server4	Terminal Server	Hourly 24-hrs day	30 Rolling Days	3 Rolling Days	Update from 1 AM Nightly / SC Cloud to Hourly 24-hrs day

DEFINITIONS:

Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

Cloud Storage: A service model in which data is maintained, managed, backed up remotely, and made available to users over the Internet.

Incremental Backup: A backup containing only the files that have changed since the most recent backup (either full or incremental). The advantage of this is quicker backup times, as only changed files need to be saved. The disadvantage is longer recovery times, as the latest full backup and all incremental backups up to the date of data loss need to be restored.

Full Backup: A backup of all (selected) files on the system. In contrast to a drive image, this does not include the file allocation tables, partition structure, and boot sectors.

Disk Image: Single file or storage device containing the complete contents and structure representing a data storage medium or device, such as a hard drive, tape drive, floppy disk, CD/DVD/BD, or USB flash drive.

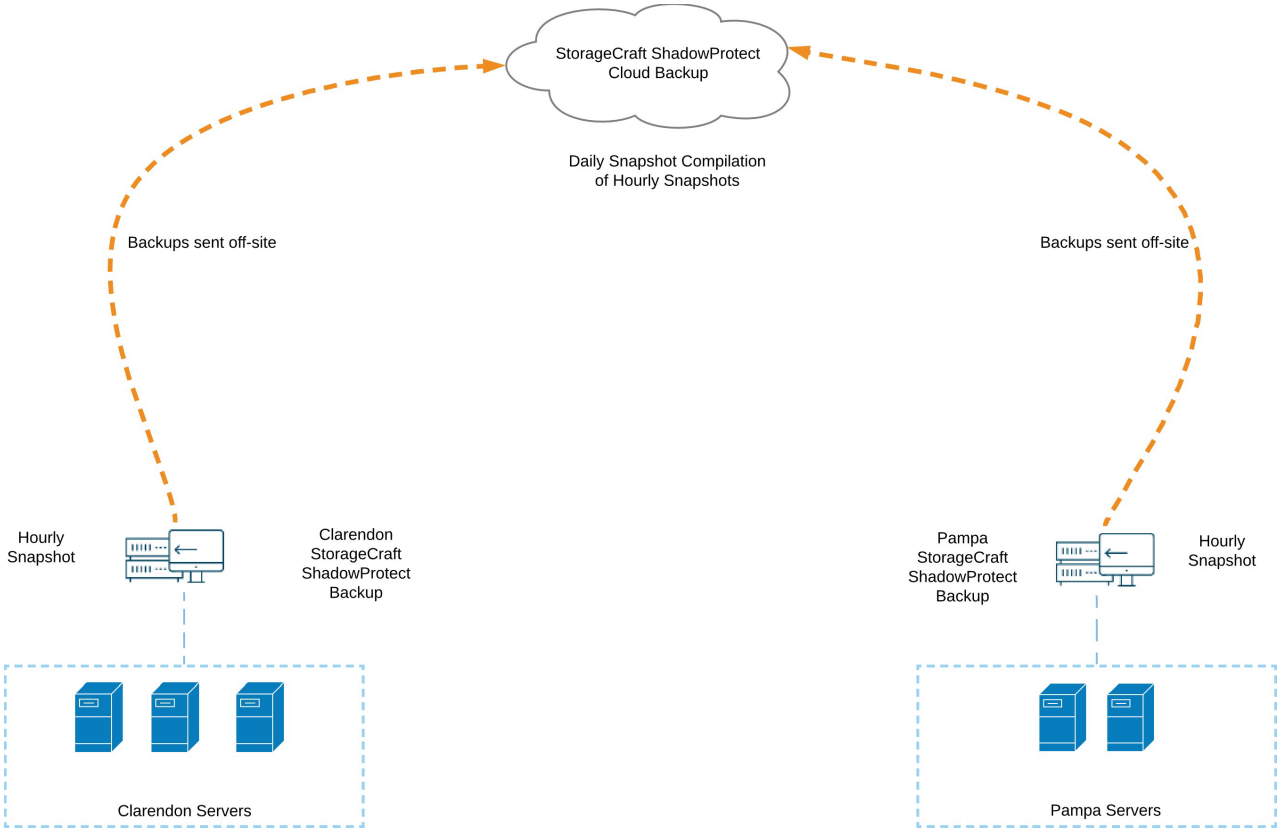
Site-to-Site Backup: Backup, over the internet, to an offsite location under the user's control. It is similar to remote backup, except that the data owner maintains control of the storage location.

Related Policies, References and Attachments:
An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at https://www.clarendoncollege.edu/information-technology.
The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on March 27, 2025, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Appendix A

The diagram below depicts a schematic diagram of the Clarendon College backup system.



The Clarendon College Board of Regents approved this policy on March 27, 2025, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Appendix B: Identification of Critical Applications

The following is a list of critical software and data for Clarendon College and its importance to date-to-date operations and backup disposition.

Importance	Application Name	Data Type	Business Impact	Backup	Sys Location	Backup Location
1	Server Systems	Virtual Server Instances	Very Critical	Yes	On-Site	On-Site/Cloud
1	CAMS Enterprise	Student Information System	Very Critical	Yes	On-Site	On-Site/Cloud
2	ED Express	Financial Aid	Critical	Yes, Data Only	On-Site	On-Site/Cloud
2	ED Connect	Financial Aid	Critical	Yes, Data Only	On Site	On Site/Cloud
3	OpenLMS	Learning Management System	Critical	Yes	Cloud	On Site/Cloud
3	Dynamics GP	Accounting	Critical	Yes	On Site	On Site/Cloud
3	Pearson Vue	Testing	Critical	Yes	On Site	On Site
4	Shared Folders	Various	Critical	Yes	On Site	On Site/Cloud
4	User Directories	Various	Critical	Yes	On Site	On Site/Cloud
5	Microsoft Office	Various	Critical	No	On Site	N/A
6	Other User Apps	Various	Moderate	No	On Site	N/A

The Clarendon College Board of Regents approved this policy on March 27, 2025, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2023.