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 use able 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. A schematic diagram of the backup process is shown on Appendix A of this policy.

POLICY STATEMENT:

1. Clarendon College-IT System Administrators are responsible for backing up Clarendon College-IT -managed servers and are required to implement a tested and auditable process to facilitate recovery from data loss.

2. All departments should store data on network storage rather than local storage (e. g. PC or Mac hard drive). Local storage is not backed up by Clarendon College-IT and will be the responsibility of the data owner.

3. Clarendon College-IT will perform timely data backups of all Clarendon College-IT managed servers containing critical data for the purposes listed above.
   a. Individual drives (redirected folders and mapped drives) and email will be retained for 30 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 vendors' 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 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, per Section D at a Classification Policy (). Data identified by the Data Owner as non-critical may be excluded from this policy.
   a. Alternative backup schedules and media management maybe 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 data location that is physically different from the original data source.
7. Verification, through restoration of backed-up data, must be performed on a regular basis as defined by the Clarendon College-IT back-up procedures document for the respective system.
8. Procedures for backing up of critical data and the testing of 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 to be used (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 that are 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. 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 (IP).

9. Backup Schedule

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

Server/Host	Data Description	Recovery Points	Local Retention	Offsite Retention	Offsite Replication
Server1	Accounting Database (GP/SQL)	Hourly from 9AM-9PM	30 Rolling Days	3 Rolling Days	1 AM Nightly / SC Cloud
Server2	File shares	Hourly from 9AM-9PM	30 Rolling Days	3 Rolling Days	1 AM Nightly / SC Cloud
Server3	AD / Security	Hourly from 9AM-9PM	30 Rolling Days	3 Rolling Days	1 AM Nightly / SC Cloud
Server4	Terminal Server	Hourly from 9AM-9PM	30 Rolling Days	3 Rolling Days	1 AM Nightly / SC Cloud

DEFINITIONS:

Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department that has the responsibility for maintenance and supervision of the Clarendon College IT infrastructure.

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

Incremental Backup: A backup that only contains 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. Similar to remote backup except that the owner of the data maintains control of the storage location.

Related Policies, References and Attachments:

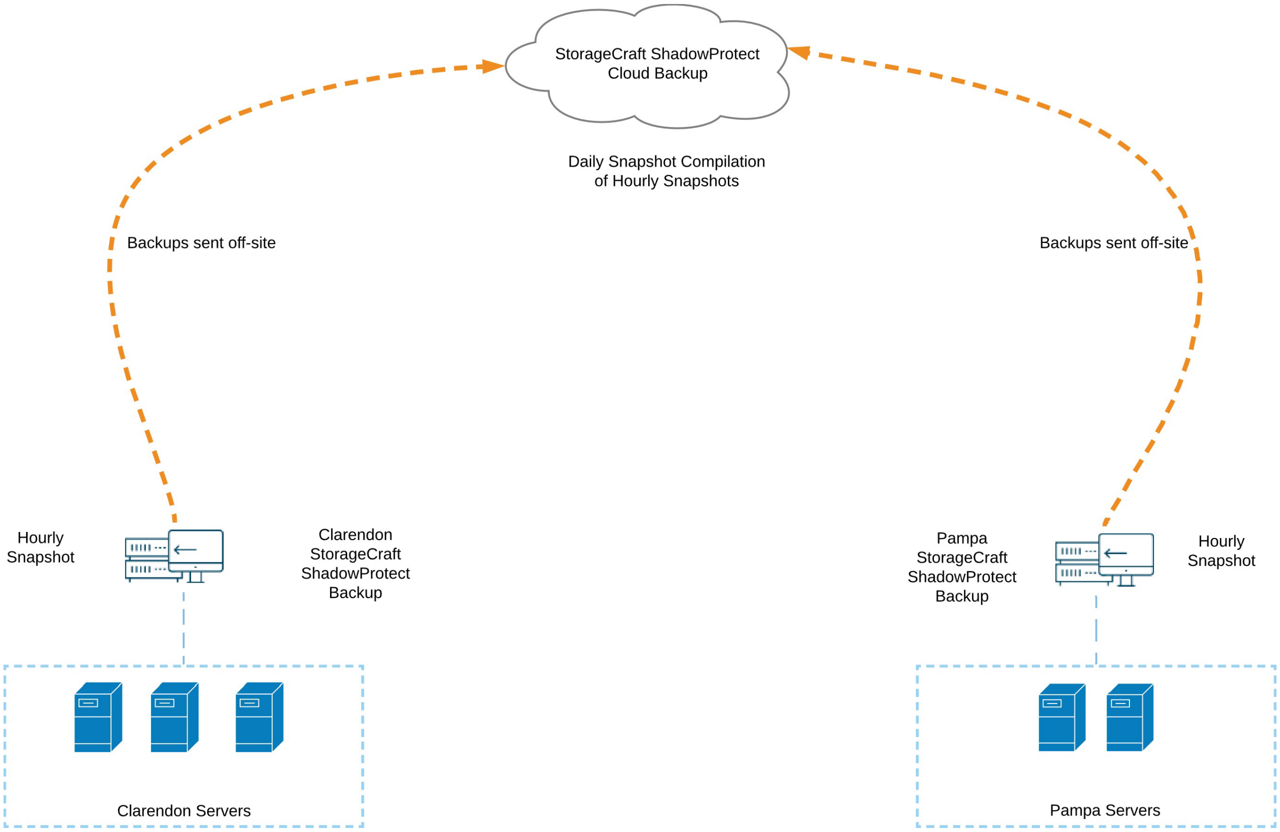
An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at https://www.clarendoncollege.edu/information-technology.

Reference materials, legal compliance guidelines, and policy enforcement are available in the Policy Compliance Document. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

This policy was approved by the Clarendon College Board of Regents on July 17, 2023, version1.1. This policy was reviewed by Will Thompson, Vice President of IT on July 15, 2023.

Appendix A

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


StorageCraft ShadowProtect Cloud Backup
Daily Snapshot Compilation of Hourly Snapshots
Backups sent off-site
Backups sent off-site
Hourly Snapshot
Clarendon StorageCraft ShadowProtect Backup
Pampa StorageCraft ShadowProtect Backup
Hourly Snapshot
Clarendon Servers
Pampa Servers

This policy was approved by the Clarendon College Board of Regents on July 17, 2023, version1.1. This policy was reviewed by Will Thompson, Vice President of IT on July 15, 2023.

Appendix B: Identification of Critical Applications

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

Importance	Appliction 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

This policy was approved by the Clarendon College Board of Regents on July 17, 2023, version1.1. This policy was reviewed by Will Thompson, Vice President of IT on July 15, 2023.