Clarendon College

Information Technology Services (CLARENDON COLLEGE-IT)

Information Technology Change Management Policy:

PURPOSE:

Each information technology resource element occasionally requires an outage for planned upgrades, maintenance, or fine-tuning. Additionally, unplanned outages may result in upgrades, maintenance, or fine-tuning. Managing these changes is critical to providing a robust and valuable infrastructure for information technology resources.

The Information Technology Change Management policy aims to manage changes rationally and predictably so Clarendon College constituents can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce the negative impact on the user community and to increase the value of Information Technology Resources.

SCOPE:

The Clarendon College Information Technology Change Management policy applies to all individuals who install, operate, or maintain Clarendon College's information technology resources.

POLICY STATEMENT:

1. Changes to Clarendon College information technology resources, such as operating systems, computing hardware, networks, and applications, are subject to this policy. They must follow the Clarendon College-IT Change Management Procedures.

2. All changes affecting computing environmental facilities (e.g., air conditioning, water, heat, plumbing, electricity, and alarms) must be reported to or coordinated with the Information Resource Manager (IRM).

3. A Change Advisory Board (CAB) appointed by the designated IRM must regularly review change requests and ensure that change reviews and communications are satisfactorily performed.

4. A formal written change request or email must be submitted to the IRM for all scheduled and unscheduled changes. For any CAMS/Elements changes, the Change-Access-Request-Form must be used; see Appendix B.

5. For any non-CAMS changes, these are submitted directly to the IRM. These requests will use the IT_Access_Request_Form_HIPAA_PCI_FERPA Form; please see Appendix C. The IRM will review the form and, if applicable, meet with the requester and data custodians/owners for implementation.

6. All scheduled change requests must be submitted following change management procedures so that the CAB has time to review the request, determine and review potential failures, and decide whether to allow or delay the request.

7. The CAB will meet as soon as possible after a completed Change-Access-Request-Form has

been received. The CAB will assess the change's urgency and its impact on infrastructure, end-user productivity, and the budget.

8. Each scheduled Non-CAMS/Elements change request must receive formal CAB approval before proceeding.

9. The appointed IRM liaison of the CAB may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back-out plans, the timing of the change will negatively impact a key business process, or if adequate resources cannot be readily available.

10. The CAB works with the change requester to develop a specific justification for the change and to identify how the change may impact the infrastructure, business operations, and budget. The CAB uses this information to further research and develop a risk and impact analysis. When completing the change analysis, the CAB must consider the business and the technical impacts and risks.

11. System owners and/or system administrators may appeal a denied CAB change request to the IRM.

12. The IRM will convene the impacted members of the CAB, system owners, system administrators, and other stakeholders, as agreed by the IRM and System Owner(s), to decide whether to implement the requested change.

13. Customer notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures.

14. A Change Review must be completed for each change, whether scheduled or unscheduled, or successful.

15. A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:
    a. Date of submission and date of change;
    b. Owner and custodian contact information;
    c. Nature of the change; and
    d. Indication of success or failure, including lessons learned.

DEFINITIONS:

Change Advisory Board (CAB): a group comprising management and technical teams that meets regularly to review change requests.

Change Control: A formal internal control procedure to predictably manage changes so Clarendon College IT and constituents can plan accordingly.

Change Review: A method involving analyzing the problem, recommended solution, and back-out procedure. Implementation should be monitored to ensure security requirements are not breached or diluted.

Information Resources Manager (IRM): Officer responsible for managing Clarendon College's information technology resources in the State of Texas. Usually, this is the Vice President of Information Technology. If this position is vacant, it will fall to the college president.

Outage: Planned or unplanned unavailability or decrease in quality of service due to expected downtime because of upgrades, maintenance, or unexpected incidents.

System/Data Owner: Departmental position responsible for classifying business data, approving access to data, and protecting data by ensuring controls are in place.

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.html.
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, version 1.4, on May 21, 2026. This policy was reviewed by Will Thompson, Vice President of IT, on May 11, 2026.

Appendix A

Change Advisor Board Members:

1. Vice President of Information Technology
2. Vice President of Academic Affairs
3. Registrar

The Clarendon College Board of Regents approved this policy, version 1.4, on May 21, 2026. This policy was reviewed by Will Thompson, Vice President of IT, on May 11, 2026.

Appendix B: Information Technology Change Management Policy, Data Access Change Request to Electronic Information Resources

Use this form to request access to electronic files or communications as provided under Clarendon College policy (Change Management Policy).

A. REQUESTOR NAME, TITLE AND DEPARTMENT
Full Name, Title, and Department of Requestor:

B. Request access to the following data. (Must comply with Clarendon College Change Management Policy)
Please describe what module(s) will be needed.

C. Reason for request and business impact. (Must comply with Clarendon College Change Management Policy)
Please describe what you need within that module and why you need it.

D. REQUESTING PARTY/DEPARTMENT HEAD SIGNATURES
Signature of Requesting Party:_____**Date**_____ **Signature of Department Head:**_____**Date**_____ **Printed Name of Department Head:**_____

E. APPROVAL OF CHANGE REQUEST COMMITTEE (Required for All)
Access authorized?_____**Yes** _____**No** **Signature of Member 1:**_____**Date**_____ **Printed Name**_____ **Signature of Member 2:**_____**Date**_____ **Printed Name**_____ **Signature of Member 3:**_____**Date**_____ **Printed Name**_____

Change Access to Electronic Information Resources
Request Form Procedures

Policy Background:

Clarendon College highly values individual privacy and recognizes its importance in academics. The College generally prohibits access to stored electronic records and voice and data communications by anyone other than the designated owner of the computer account or electronic resource containing the information or communication or the sender or recipient of a particular communication unless the applicable owner, sender, or recipient has granted prior consent.

Clarendon College cannot guarantee the privacy or confidentiality of electronic documents. Consistent with Texas Administrative Code Chapter 202, Rule 202.75(9), users should not expect privacy when using Texas State information technology resources. Consequently, persons who use these Clarendon College-owned resources, or any personally owned device that may be connected to a Clarendon College resource, have no right to privacy in their use of these resources and devices.

However, Clarendon College will take reasonable precautions to protect the privacy and confidentiality of electronic documents and to assure persons that Clarendon College will not seek access to their electronic messages or documents without their prior consent except where necessary to:

- Satisfy the requirements of the Texas Public Information Act or other statutes, laws, or regulations;
- Satisfy other legal obligations, such as subpoenas and court orders;
- Protect and sustain the operational performance and integrity of college information systems and business processes;
- Facilitate security reviews, audits, and investigations by authorized individuals in the performance of their assigned duties;
- Allow system administrators to perform routine maintenance and operations, security reviews, and respond to emergencies;
- Allow institutional officials to fulfill their responsibilities when acting in their assigned capacity;
- Protect and support the college's and other users' legitimate interests, as the IRM and ISO determined.

Procedures for Obtaining Change Access to Electronic Records:

To appropriately preserve the privacy of electronic documents and allow authorized individuals to perform their assigned duties, specific college staff will sign a Clarendon College Data Access Change Request to Electronic Information Resources Form when requesting changes to their current data access. Employees who need to request changes to their data access will contact the Office of the Vice President of Information Technology, Information Resources Manager (IRM), by email or Teams, simply by requesting the change. The IRM will then provide the requester with the Data Access Change Request to the Electronic Information Resources Form. They will complete and submit the form to the IRM. The IRM will submit the form to the Change Access Committee for review and approval, or deny the access requests.

Individuals may request access to specific data by completing the attached Data Access Change Request Form, obtaining their organizational head's approval, and submitting the form to the Office of the Information Resources Manager (IRM). The IRM will then submit the request to the Change Access Committee for review. If the request appears to comply with college policy, the committee will coordinate with the Information Security Officer (ISO) as necessary to fulfill the request. Perusal will be limited only to the areas or records that meet the criteria specified in the request.

The form will be kept on file as a record of the IRM's data access change.

The Clarendon College Board of Regents approved this policy, version 1.4, on May 21, 2026. This policy was reviewed by Will Thompson, Vice President of IT, on May 11, 2026.

Appendix C: IT Data Access and Electronic Services Request, Information Technology Change Management Policy
(Non-CAMS/Elements)

IT Data Access & Electronic Services Request Form
This form is used to request access to electronic systems, file repositories, and IT services. All requests must comply with HIPAA, PCI-DSS, and FERPA requirements, including the principle of least privilege and documented business justification.
Please check the appropriate boxes and complete fillable areas as necessary.

1. Request Type

- ☐ New Hire.
- ☐ Transfer / Role Change.
- ☐ Additional Access.
- ☐ Termination.

2. User Details

- Employee Name:
  _____
- Email Address:
  _____
- Job Title:
  _____
- Department: _____
- Manager: _____
- Location: _____
- Effective Date: _____

3. Systems & Services Requested

Please check the system or service.

- *File & Collaboration:*
  - ☐ Network Folder/Drives,
  - ☐ SharePoint,
  - ☐ OneDrive,
  - ☐ Teams,
  - ☐ Website,
    - ☐ Main Website
    - ☐ Athletic Website
    - Area of Website Requested:
      _____
  - ☐ Previous Employee Folder
    - Name of Previous Employee: _____
  - ☐ Previous Employee Email Inbox.

    - Name of Previous Employee: _____
- *Applications:*
    - ☐ EDE Express,
    - ☐ ED Connect,
    - ☐ GP (ERP),
    - ☐ Heymarket,
    - ☐ OpenLMS
        - ☐ New Shell, Course Description:
          _____
        - ☐ Access to a Previous Employee's Shell,
            - Name of Previous Employee:
              _____
    - ☐ SFTP,
    - ☐ Tawk.To,
    - ☐ Testing,
    - ☐ Signage System,
    - ☐ Other:
      _____
- *Security & Connectivity:*
    - ☐ VPN,
    - ☐ MFA,
    - ☐ Email Distribution Lists, Name:
      _____
    - ☐ Security Camera,
    - ☐ New Phone Number,
        - ☐ Need a desk phone
    - ☐ Forward Previous Employee Calls to my number,
        - Previous Employee Number: _____
    - ☐ New Fax Number.

4. Access Details

Please describe the name of the resource that is being requested in Item 3.

- Resource Name / Path:
  _____
- Access Level:
    - ☐ Read
    - ☐ Modify
    - ☐Admin
- ☐ Permanent Access
- ☐ Temporary Access (include end date): _____

5. Business Justification

- Explain why access is required and how it supports job duties (required for HIPAA/PCI/FERPA compliance):

6. Data Classification

- ☐ Public
- ☐ Internal
- ☐ Confidential
- ☐ Regulated (PHI / PII / PCI / Student Records)

7. Approvals

- Manager's Approval
  - Name: (print) _____
  - Signature: _____
  - Date: _____
- Data Custodian Approval:
  - Name: (print) _____
  - Signature: _____
  - Date: _____
- IT Security Review:
  - Name: (print) _____
  - Signature: _____
  - Date: _____
- Completion Date: _____

The Clarendon College Board of Regents approved this policy, version 1.4, on May 21, 2026. This policy was reviewed by Will Thompson, Vice President of IT, on May 11, 2026.