**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.

5. 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.

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

7. Each scheduled change request must receive formal CAB approval before proceeding.

8. 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.

9. The CAB works with the change requestor 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.

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

11. 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.

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

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

14. 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 comprises management and technical teams that meet 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 the State of Texas managing Clarendon College's information technology resources. 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 or 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.
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**

**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 on March 27, 2025, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.