Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
System Development & Acquisition Policy:

PURPOSE:
The System Development & Acquisition Policy aims to ensure that security is integral to Clarendon College system planning and management and the business processes associated with those systems.

The procedures for new and changed information systems that contain protected data must integrate information security requirements into the software lifecycle. The security requirements must identify controls to ensure confidentiality, integrity, and availability. These controls must be appropriate and cost-effective and mitigate risks resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the protected data. This is true regardless of whether the systems are purchased, used from community or open-source collaborations, or developed by Clarendon College.

SCOPE:
The System Development & Acquisition Policy applies to all software/systems installed and utilized on Clarendon College information technology resources that contain confidential and/or protected data.

This policy does not apply to faculty or students developing and experimenting with software programs as part of an approved curriculum.

POLICY STATEMENT:
All in-house software that runs in a production environment shall be developed according to the Clarendon College-IT Project Lifecycle Policy and must adhere to the Clarendon College Application Security Policy. At a minimum, this plan shall address the areas of stakeholder identification and involvement, preliminary analysis or feasibility study, risk identification and mitigation, systems analysis, general design, detail design, development, quality assurance and acceptance testing, implementation, and post-implementation maintenance and review. The requirement for such methodology ensures that the software will be adequately documented and tested before it is used for critical information. Additionally, this methodology ensures that projects match the College's strategic direction and comply with guidelines.

Where resources permit, there shall be a separation between the production, development, and test environments. This ensures that security is rigorously maintained for the production system while the development and test environments can maximize productivity with fewer security restrictions. Testing should not be performed using production systems due to the threat to its confidentiality and/or integrity.

All applicable systems shall have designated owners and custodians. Clarendon College-IT shall perform periodic risk assessments of production systems to determine whether the controls employed are adequate.

If an enterprise information system or component of that system is acquired from an external vendor, written documentation must be provided that specifies how the product meets the security requirements of this policy and any special security requirements of the system. The vendor must allow Clarendon College to test the system's security controls if needed. All acquired software that runs on production systems shall be subject to the Clarendon College-IT Project Lifecycle and must adhere to the Clarendon College Application Security Policy.

An assessment of the system's security controls and a vulnerability assessment must be performed on all new information systems or systems undergoing significant change before moving them into production. Periodic vulnerability assessments must also be performed on production information systems, and appropriate measures must be taken to address the risk associated with identified vulnerabilities.

Clarendon College-IT Change Management Policy will be followed to review and approve a change before it is moved into production.

Opportunities for misuse of information should be appropriately minimized or prevented with risk assessments, monitoring and logs, and end-user awareness and training on preventive strategies.

DEFINITIONS:
Change Management: The controlled identification and implementation of required changes within a business's information technology systems.

Data Custodian: The person responsible for overseeing and implementing physical, technical, and procedural safeguards specified by the data owner.

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

Project Lifecycle: A series of activities to fulfill project goals or objectives.

Risk Assessment: A systematic process of identifying, evaluating, and estimating the risks involved in a process or system, their comparison against benchmarks or standards, determining appropriate ways to eliminate or control the hazard, and determining an acceptable level of risk.

System Development & Acquisition: An organization's ability to identify, acquire, install, and maintain appropriate information technology systems. This includes internally developing software applications or systems and purchasing hardware, software, or services from third parties.

Stakeholder: A person or group interested in something, is impacted by it, and cares about how it turns out.

Vulnerability Assessment: Identifying, quantifying, and prioritizing a system's vulnerabilities (weaknesses).

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.

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 18, 2025.