Clarendon College
System Information Technology Services (CLARENDON COLLEGE-IT)
IT Risk Assessment Policy:

PURPOSE:
IT risk assessments are designed to assess the security posture of a system or application to ensure management's awareness of the significant security risks in the Clarendon College infrastructure and recommend mitigation plans for these risks.

The principal goal of a risk management process is to protect the College and its ability to perform its mission. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system but as an essential management function of the College.

Risk assessments will be conducted annually, as directed by the state, and/or on an ad-hoc basis in response to specific events, such as when significant modifications are made to the system's environment or in response to a security incident or audit.

SCOPE:
The Clarendon College Risk Assessment Policy applies to all stakeholders involved in preserving the confidentiality, integrity, and availability of information technology resources. Stakeholders include, but are not limited to, Clarendon College administration, application administrators, system administrators, data owners, users, and information security personnel.

POLICY STATEMENT:
Appropriate security levels and data control requirements must be determined for all information technology resources based on Clarendon College confidentiality, integrity, and availability requirements for the information, as well as its criticality to Clarendon College's mission and legal requirements.

Information technology risk analysis and management processes require gathering a broad range of data on information technology assets and potential threats. The data collection phases of the risk management process include an information technology asset inventory consisting of server build documentation, network penetration tests, logs, patch histories, and other vulnerability assessment tools for essential assets.

The ISO shall periodically (at least annually) complete or commission a risk assessment of the information resources considered essential to the College's critical mission and functions. It shall recommend appropriate risk mitigation measures, technical controls, and procedural safeguards to the owners and custodians of these resources.

The assessment may incorporate self-assessment questionnaires, vulnerability scans, scans for confidential information, and penetration testing. Findings and recommendations shall be provided to the owners and custodians of the information assets. They shall also be presented to the Vice President of Information Technology and members of the IT Governance Committee for sharing with the president as appropriate.

The key roles of personnel who are responsible for the protection of Clarendon College information technology resources and participate in the risk management/assessment process can be found in the Clarendon College Information Security Program at Information Security Program. Roles include Data Owner or designated representative(s), Data Custodian(s), Users, Information Security Officer (ISO), and Information Resources Manager.

DEFINITION:
Network Penetration Test: A pen test is an authorized simulated attack on a computer system that looks for security weaknesses, potentially gaining access to the system's features and data.

IT Governance Committee: A group that oversees an organization's IT strategy, systems, financing, and risk management. The committee's role is to ensure the organization’s IT investments align with its goals. A committee consisting of the President, Vice President of Academic Affairs, and the Vice President of Information Technology.

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.