Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Intrusion Detection/Prevention and Security Monitoring Policy:

PURPOSE:
The Clarendon College Information Security Officer is charged with securing all Clarendon College owned information technology resources, both centralized and decentralized, and has the responsibility and College-wide authority to monitor the use of information technology resources to confirm that security practices and controls are in place, are effective, and are not being bypassed.

The purpose of the Intrusion Detection/Prevention and Security Monitoring Policy is to outline College policy regarding the monitoring, logging and retention of network packets that traverse Clarendon College networks, as well as observe events to identify problems with security policies, document existing threats and evaluate/prevent attacks.

Intrusion Detection and Prevention systems focus on identifying possible incidents, logging information about them, and reporting attempts to security administrators. It plays an important role in implementing and enforcing security policies.

Clarendon College takes reasonable measures to assure the integrity of private and confidential electronic information transported over its networks and to detect attempts to bypass the security mechanisms of information resources. This will allow for early detection of wrongdoing, new security vulnerabilities, or new unforeseen threats to information technology resources, thus minimizing the potential harmful impact.

Protecting sensitive information and mitigating risks to the college's network infrastructure are paramount for several reasons:

1. **Preservation of Privacy:** Students, faculty, staff, and other stakeholders entrust the college with their personal and sensitive information. Safeguarding this data is essential for preserving their privacy and maintaining trust in the institution.
2. **Legal Compliance:** The college is subject to various laws and regulations governing the protection of sensitive information, such as the Family Educational Rights and Privacy Act (FERPA) in the United States. Failure to comply with these regulations can result in legal penalties, financial liabilities, and damage to the college's reputation.
3. **Intellectual Property Protection:** The college can often possess valuable intellectual property, including research data, proprietary software, and innovative ideas developed by faculty and students. Protecting this intellectual property from unauthorized access, theft, or tampering is critical for maintaining the institution's competitiveness and fostering a culture of innovation.

4. **Continuity of Operations:** Disruptions to the college's network infrastructure, whether due to cyberattacks, data breaches, or other security incidents, can disrupt normal operations, compromise academic activities, and impede the delivery of essential services. Mitigating risks to the network infrastructure helps ensure the continuity of operations and minimizes the impact of potential disruptions.
5. **Financial Stability:** Security incidents can have significant financial implications for the college, including remediation costs, legal expenses, regulatory fines, and loss of revenue or funding. By proactively protecting sensitive information and mitigating risks to the network infrastructure, colleges can avoid costly security breaches and preserve their financial stability.
6. **Reputation Management:** Clarendon College relies on their reputation to attract students, faculty, donors, and other stakeholders. A security breach or data leak can tarnish the college's reputation, erode trust among stakeholders, and undermine its standing within the academic community. Protecting sensitive information and maintaining a secure network infrastructure are essential for safeguarding the college's reputation and credibility.

Overall, protecting sensitive information and mitigating risks to the college's network infrastructure are essential for ensuring compliance with regulations, preserving privacy, maintaining continuity of operations, safeguarding intellectual property, preserving financial stability, and protecting the institution's reputation. By prioritizing security measures and investing in robust cybersecurity practices, colleges can effectively manage these risks and safeguard their assets and stakeholders.

SCOPE:
The Intrusion Detection/Prevention and Security Monitoring Policy applies to all individuals that are responsible for the installation of new information technology resources, the operation of existing information technology resources and individuals charged with information technology resource security. Furthermore, this policy applies to all users of Clarendon College's network resources, including students, faculty, staff, and third-party contractors.

POLICY STATEMENT:
Clarendon College considers all electronic information transported over the College network to have the potential to be private and confidential. Network and system administrators are expected to treat the contents of electronic packets as such.

While it is not the policy of Clarendon College to actively monitor internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the college’s internet links. Any inspection of electronic data packets, and any action performed following such inspection, will be governed by all applicable federal and state statutes and by Clarendon College policies. Additionally, the college is committed to respecting user privacy while monitoring network activity, and any or all monitoring will occur only when necessary in accordance with applicable laws and policies.

Please refer to the Clarendon College Technology Incident Management Policy for reporting suspected or confirmed instances of intrusions or attempted intrusions.

Audit logging, alarms and alert functions of operating systems, user accounting, application software, firewalls and other network perimeter access control systems will be enabled and reviewed annually. System integrity checks of the firewalls and other network perimeter access control systems will be performed annually, see the Clarendon College Firewall Policy. All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported to the Information Security Officer.

Automated tools will provide real-time notification of detected wrongdoing and vulnerability exploitation. Where possible, a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:

- Internet traffic
- Electronic mail traffic
- Local Area Network (LAN) traffic; protocols, and device inventory
- Operating system security parameters

The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- System error logs
- Application logs
- Data backup and recovery logs
- Service desk trouble tickets and telephone call logs
- Network printer logs

Log checks and data monitoring will be reviewed quarterly depending on the risk profile of the college's network environment.

The following checks will be performed at least annually by assigned individuals:

- Password strength
- Unauthorized network devices
- Unauthorized personal web servers
- Unsecured sharing of devices
- Operating system and software licenses

Any security issues discovered will be reported immediately to the Information Security Officer (ISO).

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 May 16, 2024, version1.2.
This policy was reviewed by Will Thompson, Vice President of IT on May 9, 2024.