Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Technology Security Training Policy:

PURPOSE:
Understanding the importance of computer security and individual responsibilities and accountability is paramount to achieving organizational security goals. This will be accomplished with general computer security awareness training and targeted product-specific training. The philosophy of protection and specific security instructions must be taught to and reinforced by technology users. Security awareness and training information needs to be continuously updated and strengthened.

The purpose of the Technology Security Training Policy is to describe the requirements that ensure each user of Clarendon College's information technology resources receives adequate training in technology security issues. Additionally, state law requires that higher education institutions provide an ongoing information security awareness education program for all users of state-owned information resources (Texas Administrative Code (TAC) §202 and the following state statute: Sec. 2054.5191, Cybersecurity and Artificial Intelligence Training Required: Certain Employees and Officials.

SCOPE:
The Clarendon College Technology Security Training policy applies equally to all employees.

POLICY STATEMENT:

1. All employees, unless exempted by Section 2054.5191 and approved by the college president, must be enrolled in the Clarendon College Security Awareness Training within 30 days of initially being granted access to Clarendon College information technology resources or per the request of the data owner or supervisor. All new employees must complete their training within the first 90 days of employment or be identified as exempt.

2. All members of the Clarendon College Board of Regents will receive cybersecurity training annually.

3. Any exemption from the security training will comply with Appendix A, Clarendon College Cybersecurity Awareness Training Exemption Policy and 25% Threshold Guidance, and Appendix B, Clarendon College Cybersecurity Training Exemption Verification Form, of this policy.

4. The training year for security training will start at the beginning of the academic year, usually in the fall term.

5. The training will generally cover the following subjects: Cybersecurity Principles, Data Privacy, Malware/Phishing Security, FERPA, Clarendon College Security Policies, and

other cybersecurity topics. Nursing staff will receive additional training on HIPAA data security.

6. All non-exempted employee college emails will be subjected to phishing tests to help monitor the effectiveness of the cybersecurity training. Phishing tests will be conducted at least once per month, and the results will be recorded. Any user who fails the phishing test will be automatically enrolled in remedial cybersecurity training.

7. Every month, an email reminder will be sent to each employee who has not completed their security awareness training.

8. Annually, all employees must complete the security awareness training and pass the associated examination(s). Training must be completed by the end of May for each calendar year.

9. By the end of May, a report will be given to the college president containing the status of each employee's security awareness training.

10. An employee's failure to complete the security awareness training could result in administrative action or dismissal from employment.

11. Annually, all employees must sign a non-disclosure agreement per the Non-Disclosure Agreement Policy, stating they have read and understand Clarendon College requirements regarding Clarendon College-IT policies and procedures.

12. Clarendon College-IT must prepare, maintain, and distribute an Information Security User Guide that concisely describes Clarendon College's information security policies and procedures.

13. Clarendon College-IT must develop and maintain a communication plan that will communicate security awareness to the Clarendon College user community.

DEFINITIONS:
Information Security User Guide: Describes the requirements that ensure each person has the knowledge to protect Clarendon College's information technology resources, defend themselves, and comply with applicable laws.

Non-Disclosure Agreement: All employees must sign an acknowledgment that they have read and understand Clarendon College's computer security policies and procedures. This agreement becomes a permanent record and will be renewed annually.

Security Awareness Training: Annual training required by the Texas Administrative Code §202 to re-familiarize users with the Clarendon College policies, their responsibility to protect Clarendon College resources, and to behave responsibly, ethically, and legally.

Cybersecurity: Cybersecurity is the practice of protecting systems, networks, programs, devices, and data from digital attacks, unauthorized access, or damage. It involves a combination of technologies, processes, and, according to Cisco, people, designed to ensure the confidentiality, integrity, and availability of information.

Phishing: Phishing is a form of cyberattack and social engineering in which attackers trick individuals into revealing sensitive information—such as passwords, credit card numbers, or personal data—by impersonating a legitimate entity via emails, texts, or websites. These fraudulent messages often create a sense of urgency to steal credentials for financial gain or identity theft.

Malware: Malware, short for "**mal**icious soft**ware**," is any software intentionally designed to disrupt, damage, gain unauthorized access to, or steal data from computer systems, networks, and devices. It includes viruses, ransomware, spyware, and Trojans, often installed through phishing, malicious downloads, or system vulnerabilities.

FERPA: The **Family Educational Rights and Privacy Act**. It is a 1974 U.S. federal law that protects the privacy of student education records and applies to all educational institutions that receive funds from the U.S. Department of Education.

HIPAA: The **Health Insurance Portability and Accountability Act of 1996**. It is a US federal law designed to protect sensitive patient health information from disclosure without consent, establishing standards for electronic health records, and improving the portability of health insurance coverage.

Texas Administrative Code (TAC) §202: A state law that outlines mandatory user security practices, specifically security awareness training and non-disclosure agreements.

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

Appendix A, Clarendon College Cybersecurity Awareness Training Exemption and 25% Threshold Guidance - Technology Security Training Policy.

Purpose:
This policy establishes Clarendon College's process for identifying and exempting employees from the annual State of Texas-mandated cybersecurity awareness training when their job duties do not involve the use of a computer or computing service for at least 25% of their required work time. It ensures compliance with Texas law while recognizing that certain roles (maintenance, custodial, substitute instructors, clinical nursing staff, etc.) typically fall below this threshold.

Statutory Authority:
Clarendon College is subject to Texas Government Code § 2054.5191, which states:
"Each state agency shall identify state employees who use a computer to complete at least 25 percent of the employee's required duties. At least once each year, an employee identified by the state agency and each elected or appointed officer of the agency shall complete a cybersecurity training program certified under Section 2054.519."

The same standard applies to institutions of higher education. Employees below the 25% threshold are not required to complete the training.

Scope:
This policy applies to all Clarendon College employees (full-time, part-time, temporary, and substitute staff).

Calculation of the 25% Threshold:
The 25% threshold is based on a reasonable, good-faith assessment of the employee's actual required duties (not just job title). Texas law and the Texas Department of Information Resources (DIR) do not mandate a precise formula (e.g., no keystroke tracking required).

Common Calculation Methods:
Percentage of Work Time: Estimate the portion of a typical work week or semester spent actively using a computer for required duties. Example: An employee works 40 hours/week. If they spend approximately 10 or more hours on computer tasks (email, LMS, digital logs, etc.), that equals 25% → training is required. Under ~10 hours/week → generally exempt.

Proportion of Core Duties:
Review the job description. If roughly 1 in 4 primary duties requires computer use → likely meets the threshold.

Supervisor Assessment: Combine job description, observed activities, employee input (verified), and workload data.

Key Notes:

1. "Computer or computing service" includes desktops, laptops, tablets, college-issued smartphones, College email, College phone, Microsoft Teams, any PC application, LMS, portals, web applications, timekeeping systems, electronic or web-based records, online procurement, maintenance logs, etc.
2. Incidental use (e.g., rare clock-in on a kiosk or occasional phone check) does not count.
3. Assessment is per employee, not by title. Two people with the same title may differ based on actual duties.
4. Re-evaluate if duties change significantly during the year.
5. Documentation is required for audit/compliance (use the attached Exemption Verification Form, Appendix B).

Examples of Typically Exempt Roles (subject to individual review):

1. Maintenance, facilities, and groundskeeping staff (primarily physical work).
2. Custodial staff.
3. Substitute instructors (primarily in-person classroom/lab instruction with minimal computer-based grading or planning).
4. Clinical nursing instructors (clinical instruction).
5. If there is doubt, it is safer to require the training.

Policy Statement – Exemption Criteria:

Employees are exempt if they use a computer for less than 25% of their required duties. Exemption is documented annually via the Cybersecurity Training Exemption Verification Form. The Supervisor will request all exemptions, forward them to IT for approval, and have them accepted by the college president. Human Resources will maintain a copy of the exemption form.

Responsibilities:

1. Supervisors: Accurately assess and document the 25% threshold. All exemptions will be requested and completed by the Supervisor and forwarded to IT for approval.
2. Human Resources & Cybersecurity Coordinator: Maintain records and handle DIR compliance reporting (due annually by August 31). IT will review and approve/disapprove the exemptions. The form will then be forwarded to the college president for final review and acceptance.
3. Employees: Notify supervisor if duties change.

Compliance:

The College will certify overall compliance with DIR. Non-exempt employees who fail to complete required training may face disciplinary action. This policy will be reviewed annually.

References:

Texas Government Code § 2054.5191:
https://statutes.capitol.texas.gov/?tab=1&code=GV&chapter=GV.2054&artSec=2054.5191
DIR Statewide Cybersecurity Awareness Training page: https://dir.texas.gov/information-security/statewide-cybersecurity-awareness-training

Clarendon College Technology Security Training Policy:
https://www.clarendoncollege.edu/Resources/IT/2025/Technology%20Security%20Training%20Policy1.pdf

The Clarendon College Board of Regents approved this policy, version 1.3, on May 21, 2026. This policy was reviewed by Will Thompson, Vice President of IT, on May 11, 2026.

Appendix B: Clarendon College Cybersecurity Training Exemption Verification Form -Technology Security Training Policy

Instructions: Complete this form to document that an employee's required duties do **not** involve computer or computing service use for at least 25% of their work time. Evaluate the assessment on the job description, observed tasks, and workload. Retain for at least three years.

Section 1: Employee Information
Employee Name: _____
Job Title: _____
Department: _____
Employment Status: ☐ Full-time ☐ Part-time ☐ Temporary/Substitute

Section 2: Job Duties Assessment Brief description of primary required duties (attach job description if available):

Estimated average weekly work hours: _____
Estimated percentage of computer/computing service use:
☐ 0–10% ☐ 11–24% ☐ 25% or more (If 25%+, training required – stop here)
Justification for Exemption (check all that apply):
☐ Primarily physical/hands-on duties
☐ Primarily in-person instruction or clinical care
☐ Only incidental computer use
☐ Other: _____
Specific examples of computer use (or lack thereof):

1. _____
   (frequency/time)
2. _____
   (frequency/time)
3. _____
   (frequency/time)

Supervisor Statement: I have reviewed the duties and determined that this employee spends less than 25% of their time on computer-based tasks—exemption granted for the current review period.
Supervisor Name: _____
Title: _____
Signature: _____ Date: _____

Section 3: Review & Approval Cybersecurity Coordinator/IT Review:
☐ Approved ☐ Denied (reason: _____)
Name: _____
Signature: _____ Date: _____
Human Resources Review:
Name: _____
Signature: _____ Date: _____
College President's Acceptance:
☐ Approved ☐ Denied (reason: _____)
Name: _____
Signature: _____ Date: _____

Section 4: Notes
Re-evaluation needed if duties change? ☐ Yes ☐ No Next Review Date: _____
Additional comments: _____
Reminders: Exemption is based on actual duties, not title. Contact HR/IT with questions.

The Clarendon College Board of Regents approved this policy, version 1.3, on May 21, 2026. This policy was reviewed by Will Thompson, Vice President of IT, on May 11, 2026.