CLARENDON COLLEGE Information Security

User Guide

2025

This page is intentionally left blank.

Contents

Section 1: Introduction

1.0 Introduction

This user guide has been written to provide an easy reference for Information Security Policies associated with the CLARENDON COLLEGE Information Security Program that pertain to employee use of information technology resources. These guidelines educate individuals by summarizing acceptable practices on the essential responsibilities of utilizing information technology resources.

This Information Security Guide aims to describe the requirements that ensure everyone has the knowledge to protect CLARENDON COLLEGE information technology resources, protect themselves, and comply with applicable laws. All individuals are accountable for their actions relating to information technology resources, which are to be used for intended purposes as defined by CLARENDON COLLEGE policies and in compliance with applicable laws.

Changes to this guide will be published when available, and replacement pages or sections will be made accessible.

This guide will be provided to the Clarendon College community annually.

2.0 Overview

Information technology resources are strategic assets (procedures, software, data, equipment, and facilities used by CLARENDON COLLEGE) of Clarendon College; CLARENDON COLLEGE must manage these resources as valuable college resources. Measures will be taken to protect these assets against accidental or unauthorized access, disclosure, modification, or destruction and to assure information availability, integrity, utility, authenticity, and confidentiality.

The Texas Administrative Code Chapter 202 (TAC§202) is written for state agencies and institutions of higher education. TAC §202 defines an institution of Higher Education as; “A university system or institution of higher education as defined by §61.003, Education Code, except for public junior colleges unless otherwise directed by the Higher Education Coordinating Board (THECB)“. Clarendon College is a comprehensive, two-year community college – a public junior college. Current regulations do require CLARENDON COLLEGE to maintain compliance with TAC§202. Additionally, TAC§202 defines an outstanding security program closely following the federal requirements specified in NIST SP 800-53. Following these codes will provide security for the college’s essential data. The guidelines established in this statute will ensure that CLARENDON COLLEGE data complies with current state and federal regulations and will prepare CLARENDON COLLEGE for future compliance requirements by the THECB.

The CLARENDON COLLEGE Information Security Program and associated CLARENDON COLLEGE-IT security policies are based on the published Texas Administrative Code, Information Security Standards 1 (TAC § 202), NIST Special Publication 800-53, Security and Privacy Controls (NIST SP 800-53) and the state and federal laws and regulations listed in Policy Compliance.

This guide contains a summary of user information and responsibilities derived from the CLARENDON COLLEGE-IT security policies. For ease of inquiry, each section indicates which policy covers that topic. Policy location: https://pol.tasb.org/PolicyOnline?key=405

3.0 Applicability

This program applies equally to all individuals granted access privileges to any CLARENDON COLLEGE information technology resource. This program applies to all equipment owned or leased by CLARENDON COLLEGE or connected to the CLARENDON COLLEGE network. The *Information Security Program* applies to those that otherwise create, generate, communicate, store, process, use, and rely on information resources of the CLARENDON COLLEGE.

4.0 Users Responsibilities

1. **All individuals are personally accountable for their actions relating to information technology resources.** Users of information resources shall use college resources only for defined purposes and comply with established controls.

   Compliance with CLARENDON COLLEGE's published policies and practice standards is mandatory. As a user, your responsibility is to adequately secure information technology resources from unauthorized access, data manipulation, disclosure, and theft of sensitive and confidential information.

2. **You are responsible for knowing the regulations and policies of the college that apply to appropriate use.** Users of CLARENDON COLLEGE technology services and facilities have access to valuable college resources, sensitive data, and internal and external networks.

   You are responsible for exercising good judgment when using the college's technological and information resources.

   Just because an action is technically possible does not mean it is appropriate to perform it. Consequently, each user needs to behave responsibly, ethically, and legally.

3. **You are responsible for attending the Security Awareness Training and familiarizing yourself with the CLARENDON COLLEGE policies** available online at https://pol.tasb.org/PolicyOnline?key=405.

4. **All users must sign the CLARENDON COLLEGE Non-Disclosure Agreement (NDA),** acknowledging that they have read and understand CLARENDON COLLEGE requirements regarding computer security policies and procedures. This signed non-disclosure agreement becomes a permanent record and will be renewed annually.

5.0 Enforcement

By Policy Compliance, Violation of College policy may result in disciplinary action, including termination of employment for employees and temporary employees; a termination of contractual agreements in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion for a student. Additionally, individuals are subject to loss of Clarendon College Information Resources access privileges and possibly civil action or criminal prosecution.

Any state or federal law violations regarding these policies shall be reported to the appropriate Law Enforcement Agency.

6.0 Obtaining a Policy Exemption

Exemptions are granted on a case-by-case basis and must be reviewed and approved by the College's designated Information Resources Manager (IRM). The IRM will provide the documentation and additional administrative approvals required to consider each policy exemption request.

Section 2: User Security Practices and Safeguards

1.0 User Accounts

1. You will automatically be given an account with CLARENDON COLLEGE that you will use for any computers and/or systems you log in to. This account is unique and is to be used by you only.
2. Never share your password and USERID with anyone (including family, friends, co-workers, and supervisors).

2.0 Account Passwords

You are responsible for your account credentials, which means you are responsible for what is accessed, downloaded, or created using your credentials, regardless of intent. A person not authorized to use your credentials can cause loss of information confidentiality, integrity, and availability, resulting in liability, loss of trust, or embarrassment to CLARENDON COLLEGE.

You must create a strong password and protect it. (If you think someone has your password, the password must be changed immediately.)

1. Must create a strong password and protect it.
2. The password must have a minimum length of eight (14) alphanumeric characters.
3. Password must contain a mix of upper case, lower case, and numeric characters and special characters (!@#%^&*+=?/~';:,<>|\).
4. Passwords must not be easy to guess; for instance, they should not include part of your social security number, birth date, nickname, etc.
5. Passwords must not be easily accessible to others (e.g., posted on monitors or under keyboards).
6. Computing devices must not be left unattended without locking or logging off of the device.
7. Stored passwords must be encrypted.
8. Clarendon College username and password should not be used for external services (e.g., LinkedIn, Facebook, or Twitter).
9. Users should never share passwords with anyone, including family, supervisors, co-workers, and Clarendon College IT personnel.
10. Users must change passwords at least once every 365 days, reference NIST SP-800-63 (NIST Password Guidelines | AuditBoard).
11. If you know or suspect your account has been compromised, change your password immediately and contact Clarendon College-IT for further guidance and assistance.
12. If Clarendon College-IT suspects your account has been compromised, your account will be deactivated, and you will be contacted immediately.
13. Employees must use Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA) with their network and PC access passwords. Student use of 2FA/MFA is also encouraged.
14. Recording login information on paper notes or other unsecured means is prohibited. Using electronic password managers to store and record user login credentials is highly encouraged and is available.

3.0 Acceptable Use

Acceptable use generally means respecting other computer users' rights, the physical facilities' integrity, and all pertinent license and contractual agreements.

Acceptable Use of CLARENDON COLLEGE information technology resources is outlined in detail in the Acceptable Use Policy, as well as Data Backup, Network Use Policy, Technology Security Training Policy, Authorized Software, Electronic Communication Policy, Computer Virus (Malicious Code), and Portable Computing Policy.

All messages, files, and documents located on college information technology resources (including any personal documents) are owned by CLARENDON COLLEGE, may be subject to Open Records requests, and may be accessed by authorized CLARENDON COLLEGE CLARENDON COLLEGE-IT employees at any time without the knowledge of the information resources' user or owner.

Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet systems. Incidental use is permissible if it does not violate policy and/or exceed departmental guidelines. If you are uncertain, you should consult your supervisor.

3.0.1 Acceptable use guidelines

a. Users may use only Clarendon College information technology resources for which they are authorized.

b. Users are individually responsible for appropriately using all resources, including the computer, the network address or port, software, and hardware. They are accountable to the College for all use of such resources.

c. Authorized users of Clarendon College resources may not enable unauthorized users to access the network. The College is bound by its contractual and license agreements respecting specific third-party resources; users must comply with all such agreements when using Clarendon College information technology resources.

d. Users should secure resources against unauthorized use or access, including Clarendon College accounts, passwords, Personal Identification Numbers (PIN), Security Tokens (i.e., Smartcard), or similar information or devices used for identification and authorization purposes.

e. Users must report shareware or freeware before installing it on Clarendon College-owned equipment unless it is on the approved software list. A request to install software must be reported to the Clarendon College-IT via email before installing any software.

f. Users must not attempt to access Clarendon College information technology resources without appropriate authorization by the system owner or administrator.

3.0.2 Information Integrity

Users may not interfere with or alter the integrity of CLARENDON COLLEGE information technology resources by:

a. Impersonating other individuals in communication;

b. Attempting to capture or crack passwords or encryption;

c. Unauthorized access, destruction, or alteration of data or programs belonging to other users;

d. Use for illegal purposes, including but not necessarily limited to violation of federal or state criminal laws.

3.0.3 Internet use

a. Sensitive or confidential CLARENDON COLLEGE material transmitted over external networks shall be encrypted.

b. User activity on CLARENDON COLLEGE information technology resources is subject to monitoring and review.

c. CLARENDON COLLEGE reserves the right to audit networks and systems periodically to ensure compliance with this policy.

3.0.4 Electronic Communication

a. Do not send, forward, or request to receive confidential or sensitive CLARENDON COLLEGE information through or to non-CLARENDON COLLEGE E-mail accounts. (such as your account at Hotmail®, Yahoo!® mail, Google mail (Gmail), etc.)

b. Confidential data must be protected at all times from unauthorized disclosure. Encryption is an acceptable method of data protection.

3.0.5 Portable Computing

The users of portable computing devices or media used to store, transmit, or process protected data are expected to take all appropriate measures and precautions to prevent the loss, theft, damage, and/or unauthorized use and shall include the following:

a. All reasonable precautions to prevent data compromise should be taken when using portable computing devices (e.g., shield screen from passive viewing, password-protected screen saver).

b. Ensure the device is shut down or secured when not in use (e.g., password-protected devices offering such capabilities).

c. Physically safeguard the devices. Keep portable computing devices within view or securely stored at all times. Unattended portable computing devices must be physically secure (e.g., locked in an office, desk drawer, or filing cabinet; in an automobile, safe in a non-visible location).

d. Use encryption to safeguard all storage media (e.g., hard drives, USB flash drives, flash memory cards).

e. Confidential information should not be stored on a portable computing device.

f. Do not allow unauthorized persons to access CLARENDON COLLEGE portable computing devices or media. **You are responsible for any misuse of the information by persons to whom you have given access.**

g. Promptly notify CLARENDON COLLEGE-IT if any portable computing device or media has been lost or stolen.

3.0.6 Technology Security Training

a. All employees must complete the CLARENDON COLLEGE security awareness training class within 30 days of being granted access to any CLARENDON COLLEGE information technology resources and pass the associated examination.

b. All employees must complete the security awareness training annually and pass the associated examination to reinforce knowledge of technology security issues.

c. All employees will review, sign, and return the Clarendon College Non-Disclosure Agreement.

3.0.7 Computer Virus (Malicious Code)

a. All workstations and laptops must use college-approved virus protection software and configuration.

b. The settings for the virus protection software must not be altered to reduce the frequency of updates or bypass or turn off the software.

c. Viruses not automatically cleared by the virus protection software are security incidents and must be reported to Information Technology Services at (806) 874-4816 or administrator@CLARENDONCOLLEGE.edu.

3.0.8 Data Backup

Electronic backups are a business requirement to recover data and applications in the case of natural disasters, system disk drive failures, espionage, data entry errors, or system operations errors.

a. Any data used in an information technology resource system must be kept confidential and secure by the user.

b. All departments should store data on network storage (e.g., “My Documents” drives) rather than local storage (e.g., PC or Mac hard drive). **CLARENDON COLLEGE-IT does not back up local storage.**

c. CLARENDON COLLEGE IT System Administrator will provide backups and one-month retention of data that has been determined critical (SQL data is retained for 60 days).

d. Records retention is the responsibility of your department’s data owner. Suppose files need to be retained beyond the one-month archive. Those files must be kept in the network storage area and included in regular backups or separately archived by the data owner for permanent retention.

3.0.9 Authorized Software

Users shall accept the responsibility to prevent illegal software usage and abide by college policy on using copyrighted materials, requiring the college community to respect copyright law.

These responsibilities include:

a. Do not illegally distribute or share software with anyone.
b. All software must be license-compliant, including personally purchased software.
c. CLARENDON COLLEGE-IT must install all software unless prior arrangements have been made.
d. All software licenses must be readily available.
e. Report any suspected or known misuse of software to CLARENDON COLLEGE-IT Client Support Services.

You should not expect personal privacy concerning CLARENDON COLLEGE information technology resources. Information technology resources provided by CLARENDON COLLEGE are owned by Clarendon College and subject to CLARENDON COLLEGE oversight. Electronic files and communication created, sent, received, or stored on CLARENDON COLLEGE information technology resources are not private and may be subject to open records requests.

CLARENDON COLLEGE information technology resources may be monitored to manage performance, perform routine maintenance and operations, protect the integrity of CLARENDON COLLEGE information technology resources, perform security reviews, and fulfill complaint or investigation requirements. For these same purposes, CLARENDON COLLEGE-IT may also capture user activity, such as visiting websites.

4.0 Privacy

CLARENDON COLLEGE Internal Privacy:

Electronic files created, sent, received, or stored on computers owned, leased, administered, or otherwise under the custody and control of Clarendon College are the property of Clarendon College. These files are not private and may be accessed by authorized Clarendon College-IT employees and campus administration at any time without the knowledge of the information technology resource user or owner.

To manage systems and enforce security, Clarendon College-IT may log, review, and otherwise utilize any information stored on or passing through its information technology resource systems under the provisions and safeguards provided in the Texas Administrative Code § 202 (TAC § 202), Information Resource Standards. For these same purposes, Clarendon College-IT may also capture user activity, such as visiting websites. Third-party and customer information has been entrusted to Clarendon College for business purposes, and all faculty and staff will do their best to safeguard the privacy and security of this information. Customer account data is confidential, and access will be limited based on business needs.

CLARENDON COLLEGE Website Public Privacy:

Clarendon College maintains the http://www.clarendoncollege.edu/ website and other Clarendon College-owned or –hosted domains as a public service. Clarendon College's detailed public privacy statement (Web Privacy and Site Link) regarding individual websites, data collection, public forums, and links to other sites is available on the website (Web Privacy and Site Link).

For site management functions, information is collected for analysis and statistical purposes (please

refer to CLARENDON COLLEGE Web Privacy and Site Link Policy). This information is not reported or used in any manner that would reveal personally identifiable information unless Clarendon College is legally required to do so in connection with law enforcement investigations or other legal proceedings.

For site security purposes and to ensure that the site remains available to all users, Clarendon College uses software to monitor network traffic to identify unauthorized attempts to upload or change information or otherwise cause damage, which is strictly prohibited and may be punishable under applicable state and federal laws.

5.0 Physical Security

All information technology resource facilities will be physically protected in proportion to the criticality or importance of their function at CLARENDON COLLEGE.

1. Access to information technology resource facilities must be granted only to CLARENDON COLLEGE support personnel and contractors whose job responsibilities require access to that facility, and physical access must be documented and managed.
2. Access cards and/or keys must not be shared or loaned to others.
3. Access cards and/or no longer required keys must be returned to the person responsible for the college facility.
4. Visitors must be escorted in card access controlled areas of information technology resource facilities, and visitors will be tracked with a sign-in/out log.

Section 3: FAQ

1. **What are my responsibilities as a CLARENDON COLLEGE information technology resource user?**

   a. Be accountable for your actions regarding technology
   b. Protect CLARENDON COLLEGE information technology resources by following policies and exercising good judgment.
   c. Know the regulations and policies of CLARENDON COLLEGE
   d. Take the initial and annual security awareness training
   e. Sign the non-disclosure agreement

2. **Why does my computer have a screensaver timeout?**

   The law dictates we all must protect CLARENDON COLLEGE data. If you do not lock your computer when not in use, a universal security feature will lock it for you after a predetermined amount of time, assuming you have left it unattended and unprotected.

3. **Why does my password have to be so complicated?**

   The more complex your password, the less likely someone will guess or hack your password and cause damage to CLARENDON COLLEGE resources in your name, leaving you responsible for the damage.

4. **Why can't I create CLARENDON COLLEGE documents on a personal Google Docs or Office 365 account?**

   Storing CLARENDON COLLEGE documents that could potentially be sensitive or confidential on a public server is an example of using bad judgment in protecting CLARENDON COLLEGE data. Public servers can be compromised, and CLARENDON COLLEGE-IT has no control over safeguarding that data.

5. **Is it OK to forward my CLARENDON COLLEGE email to my home email account?**

   No, any CLARENDON COLLEGE email has the potential to contain confidential information. Once the email leaves the security of the CLARENDON COLLEGE network, it will pass through several public servers as it is routed to your home email, leaving a copy of that email on each unsecured routing server. The CLARENDON COLLEGE confidential information will also be compromised when that public server is compromised.

6. **Can I take CLARENDON COLLEGE documents home on my flash drive to work on at home?**

   It is discouraged. You must encrypt the drive to protect the data if you have no choice. When in doubt about the level of confidentiality, err on the side of sound judgment and encrypt it. Ask yourself if that information would be ok to be read by anyone if it ended up on the front page of a national newspaper.

7. **I have this great program from home; can I load it on my CLARENDON COLLEGE PC?**

   All software must be approved and installed by CLARENDON COLLEGE-IT. There are factors to be considered, such as licensing, compatibility, etc. Call the service desk to determine whether it meets the criteria.

8. **Is it ok to access social networking on my college computer?**

   CLARENDON COLLEGE blocks employee social networking sites on Clarendon College IT systems. Use of social networking sites during work hours is discouraged.

9. **I've lost a CLARENDON COLLEGE device (phone, laptop, iPad, etc.); what do I do now?**

   Immediately notify your supervisor and call the service desk. They will initiate the proper process for informing the Information Security Officer, who will notify law enforcement if theft is involved.

10. **I have accidentally deleted files on my local PC (or laptop); can you restore them?**

    Maybe it depends on where you saved the file. They are achieved if you save the file in the My Documents folder. If they are in any other folder, they are not backed up. Remember, backups are performed in case of natural disasters, system disk drive failures, espionage, data entry errors, or system operations errors. Restoring a single file or email is a significant undertaking, so take care when deleting files.

11. **I was perusing the network drive and came upon employee evaluations. Can I read them since they're available to me?**

    These are categorized as confidential files and should not be accessible to you. Call the helpdesk if this happens, as they will need to initiate the process of informing the systems administrators to correct the error.

12. **Can I print my recipes on a CLARENDON COLLEGE color printer?**

    Remember that your personal use must not result in direct costs to CLARENDON COLLEGE. The cost of paper, toner, and wear and tear on the printer is a cost to CLARENDON COLLEGE.

13. **What's wrong with keeping my vacation pictures or music files in the My Documents folder?**

    a. You do not want others viewing your pictures for many reasons, including if someone considers them inappropriate.
    b. You are allocated a specific amount of server storage space. If you run out of storage, systems administrators may delete pictures or music files to clean it up.
    c. The storage space on the server and the backup tapes that your pictures use result in direct costs to CLARENDON COLLEGE.

14. **I don't like the thought of someone from IT reading my documents on my "My Documents" drive; what can I do?**

    Do not store personal documents on the server.

15. **My co-worker used my PC while logged in as me, and I was away from my desk; they sent a scathing email to the College President, asking why I was in trouble.**

    It is your responsibility to protect the information you have access to; locking your machine when you leave your workstation is vital to that protection.

16. How was I supposed to know I was supposed to call the service desk if I saw that my anti-virus didn't get rid of that virus?

You are responsible for knowing and understanding the policies that govern the use of CLARENDON COLLEGE information technology resources. This is why familiarizing yourself with CLARENDON COLLEGE policies and attending security awareness training is imperative.

Section 4: Glossary

Glossary

This glossary contains an alphabetized listing of both standard and specific terms that are used in the **INFORMATION SECURITY USER GUIDE**.

CONFIDENTIAL INFORMATION

Information maintained by CLARENDON COLLEGE that is exempt from disclosure under the provisions of the Texas Public Information Act (*also known as* the Texas Open Records Act) or other state or federal law is confidential.

ELECTRONIC COMMUNICATION

Electronic communication transfers text, HTML, images, or data through a computer, cell phone, tablet, PDA, or other communication device. This includes E-mail, instant messaging, texting, web pages, blogs and forums.

ENCRYPTION (ENCRYPT, ENCIPHER, OR ENCODE)

The conversion of plaintext information into a secret code concealing the data's original meaning cannot be understood by anyone but the intended recipient.

FLASH DRIVE

For a small data storage device with flash memory and a built-in universal serial bus (USB) connection, flash drives typically have no more than two or three inches long and less than an inch wide.

FLASH MEMORY CARD

A solid-state electronic flash memory data storage device. These are mainly used with digital cameras, handheld and mobile computers, mobile phones, music players, digital cinematography cameras, video game consoles, and other electronics.

INCIDENTAL USE

The personal use of the internet on state networks occurs in incidental amounts of employee time, such as during reasonable convenience breaks.

INFORMATION TECHNOLOGY RESOURCES

Any computer printouts, online display devices, magnetic storage media, and all computer-related activities involving a device capable of receiving e-mail, browsing websites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (**PDA**s), pagers, distributed processing systems, network attached and computer-controlled medical and laboratory equipment (e.g., embedded technology), telecommunications resources, network environments, telephones, fax machines, printers, and service bureaus.

INFORMATION RESOURCE MANAGER (IRM)

The individual is responsible to the State of Texas for managing the college's information technology resources. The IRM has been given the authority and the accountability by the State of Texas to implement security policies, procedures, practice standards, and guidelines to protect CLARENDON COLLEGE information technology resources.

INFORMATION SECURITY OFFICER (ISO)

The employee is responsible for administering the information security functions within the college. The ISO is the college's internal and external point of contact for all information security matters.

INTERNET
A global system interconnecting computers and computer networks. The computers and networks are owned separately by various organizations, government agencies, companies, and colleges.

INTRANET
An organization's network (internal internet) is accessible only by the organization's employees or others with authorization. An intranet's website looks and acts just like any other website but is protected from unauthorized access by a firewall.

LOCAL AREA NETWORK (LAN)
A communications network that serves users within a confined geographical area. It comprises servers, workstations, a network operating system, and a communications link.

PASSWORD
A string of characters that authenticate a person's identity and may be used to grant or deny access to private or shared data.

PORTABLE COMPUTING DEVICE
Any portable device capable of receiving and/or transmitting data to and from information technology resources. These include, but are not limited to, notebook computers, handheld computers, PDAs (personal digital assistants), pagers, cell phones, Universal Serial Bus (USB) drives, memory cards, external hard drives, data disks, CDs, DVDs, and similar storage.

VIRUS
A program that can replicate itself spreads from one computer to another and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed.

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.