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

PURPOSE:
This policy is intended to ensure that all Clarendon College personnel are aware of the college's responsibilities under the law.

This policy governs the actions of any Clarendon College official (defined below) who discovers or is notified of a breach or possible breach of the security of unencrypted personal information collected and retained by Clarendon College as computerized data.

This document establishes specific requirements for the use of all computing and network resources at Clarendon College. (See Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC§202) and Texas Higher Education Coordinating Board)

This policy should be used along with the Clarendon College Technology Incident Management Policy.

SCOPE:
This breach can be the result of a compromise of a Clarendon College computing system or network, the loss or theft of any physical device in which personal information is stored, or the loss or theft of any storage medium upon which personal information is maintained.

Clarendon College maintains computerized data on various college systems which includes personal information. If the security of any Clarendon College system storing or processing computerized data that includes unencrypted personal information is compromised, the owner or licensee of that information must be notified by the college of the breach of the system if the information was, or is reasonably believed to have been, acquired by an unauthorized person.

RIGHTS AND RESPONSIBILITIES:
Good faith acquisition of personal information by a Clarendon College official with a legitimate educational interest in the data or information is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure. Clarendon College is not required to disclose a technical breach of system security which does not seem reasonably likely to subject the owners of personal information stored on those systems to a risk of criminal activity.

All college officials have a duty to comply with and to understand their responsibilities as expressed in this policy. Certain Clarendon College administrative personnel also have additional responsibility for maintenance and for execution of this policy.

POLICY STATEMENT:

1. This disclosure shall be made as expediently as possible following discovery or notification of the breach—without unreasonable delay and consistent with any measures taken to determine the scope of the breach and restore the integrity of the affected data system. This notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. In that case, the notification may be made after the law enforcement agency determines that such notification does not compromise an ongoing investigation.
2. Any college official who discovers or is notified of a breach of the security of any Clarendon College technology system will report it. The initial report of a potential security breach involving computerized data will likely be made in one of three ways:
    a. A report to the Clarendon College Vice President of Information Technology of the theft of a computing or storage device.
    b. If the presenting incident is a theft, the Vice President of Information Technology will:
        i. Report it to law enforcement, and act as liaison with any law enforcement agency involved in the situation;
        ii. Notify the Dean of Administrative Services of the incident, and
        iii. Notify the Vice President of Academic and Student Affairs (or designee) of the incident.
        iv. Follow normal computing services inventory procedures regarding loss or theft of technology;
3. The discovery of a breach of security of a computer or the Clarendon College network by support staff.
    a. If the presenting incident is discovery of a network breach, the Vice President of Information Technology will:
        i. Begin network and computer technical investigations following the guidelines articulated in the Clarendon College IT security standard addressing intrusion detection and incident response. This will continue until the security and technical aspects of the situation are resolved.
        ii. Notify the Dean of Administrative Services of the incident, and
        iii. Notify the Vice President of Academic and Student Affairs (or designee) of the incident.
4. In some circumstances, it may be appropriate to report a breach of the security of the network or Clarendon College computers to law enforcement, as well.
    a. The Vice President of Information Technology (or designee) and the Dean of Administrative Services (or designee) will consult regarding the nature and scope of the security breach and to determine whether law enforcement needs to be notified.
    b. The Vice President of Information Technology (or designee) will notify the Vice President of Academic and Student Affairs (or designee) regarding the incident and will have responsibility for guiding the initial investigation by IT technical representatives into the situation and determining the nature of any unencrypted data which may have been compromised.
5. If it is determined that a breach may have compromised the security, confidentiality, or integrity of Clarendon College-managed personal information, the Vice President of Academic and Student Affairs (or designee) will initiate a meeting as soon as possible of the college's Incident Response Team, consisting of the following or their designees:

a. Vice President of Academic and Student Affairs (chair).
b. Vice President of Administrative Services.
c. Registrar (if student data may be involved) and/or Payroll/Benefits Coordinator (if staff data may be involved).
d. Vice President of Information Technology.

6. The Dean of Administrative Services will notify the president of the college that the Incident Response Team has been activated and will provide updates regarding actions taken, as appropriate.
7. The Incident Response Team will:
    a. Assign from the team membership a scribe responsible for maintaining notes, minutes and a final written report to the college president regarding the incident, its resolution and the institutional response.
    b. Gather information regarding the situation and the type and nature of the unencrypted data that has potentially been compromised.
    c. Determine if a legal responsibility exists to notify individuals that their personal information has or may have been disclosed.
    d. Determine who is affected by the breach and should be notified.
    e. Determine which of the methods of disclosure (below) prescribed by law is appropriate.
    f. Assign appropriate tasks to team members based on their institutional responsibilities and expertise. These tasks will be determined by the team based on the specific situation.
    g. Conduct a debriefing meeting once the situation is resolved to review and approve the report to the college president.
8. Notification of disclosure of personal information may be made in one of the following methods:
    a. Written notice.
    b. Electronic notice consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec. 7001.
    c. Substitute notice. This is allowed if the cost of providing notice to all affected individuals would exceed a reasonable amount or if Clarendon College does not have sufficient contact information. Substitute notice is defined as ALL of the following:
        i. E-mail notice when Clarendon College has an e-mail address for the subject persons,
        ii. Conspicuous posting of a notice on Clarendon College's web site, and
        iii. Notification to major statewide media.

DEFINITIONS:

College Official: Clarendon College defines a college official as:

1. A person employed by the college in an administrative, supervisory, academic or research, or support staff position.
2. A person appointed to the board of regents.
3. A person assigned, employed by or under contract to the college to perform a special task, such as an attorney or auditor.
4. A person who is employed by public safety.

5. A student serving on an official committee, such as a disciplinary or grievance committee, or who is assisting another college official in performing his or her tasks.

Legitimate Educational Interest: Clarendon College defines a college official who has a legitimate educational interest as one who is:

1. Performing a task that is specified in his or her position description or contract agreement.
2. Performing a task related to a student's education.
3. Performing a task related to the discipline of a student.
4. Providing a service or benefit relating to the student or student's family, such as health education, Counseling, advising, student employment, financial aid, or other student service related assistance.
5. Maintaining the safety and security of the campus.
6. Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department that has the responsibility for maintenance and supervision of 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. 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 July 17, 2023, version1.1. This policy was reviewed by Will Thompson, Vice President of IT on July 15, 2023.