Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Technology Incident Management Policy:

PURPOSE:
The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

This document describes the requirements for dealing with computer security incidents. Security incidents include, but are not limited to: virus, worm, ransomware, spyware, and Trojan Horse detection; unauthorized use of computer accounts and computer systems; and complaints of improper use of information technology resources as outlined in the Clarendon College policies.

The policy should be used along with the Clarendon College Security Breach Notification Policy.

SCOPE:
The Clarendon College Technology Incident Management Policy applies to the ISO, IRM, and Incident Response Team (IRT).

POLICY STATEMENT:
1. As an incident is identified, pre-defined roles and responsibilities of the Clarendon College IRT members take priority over normal duties. See Appendix A, Incident Categorization and Prioritization, regarding incident priorities.
2. The ISO is responsible for initiating, completing, and documenting the incident investigation with assistance from the IRT.
3. The ISO is responsible for notifying the IRM, any company acting in behalf of the Clarendon College IT, and the IRT and initiating the appropriate incident management action including restoration as defined in the Incident Management Procedures.
4. Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed. Also see the Clarendon College Security Breach Notification Policy.
5. The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
6. The appropriate technical resources from the IRT are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
7. The ISO, working with the IRM and any company acting in behalf of the Clarendon College IT, will determine if a widespread Clarendon College communication is required, the content of the communication, and how best to distribute the communication. The appropriate technical resources from the IRT are responsible for communicating new issues or vulnerabilities to the system vendor and working

with the vendor to eliminate or mitigate the vulnerability.

8. Clarendon College-IT or any company acting in behalf of the Clarendon College IT will disconnect a server posing an immediate threat to the Clarendon College network in order to isolate the intrusion or problem and minimize risks.
    a. This can be done without contacting the owner or application administrator if circumstances warrant.
    b. The server will remain disconnected until it is brought back into compliance or is no longer a threat.
9. The Clarendon College ISO is responsible for reporting the incident to the:
    a. IRM
    b. Office of Information Technology Services as outlined in TAC§202
    c. Local, state or federal law officials as required by applicable statutes and/or regulations
10. The ISO is responsible for coordinating communications with the College media liaison.
11. In the case where law enforcement is not involved, the ISO will recommend disciplinary actions, if appropriate, to the College President.
12. In the case where law enforcement is involved, the ISO will act as the liaison between law enforcement including the College Security and Clarendon College-IT.
13. Documentation and reporting are an important part of incident management. The importance of thorough documentation and reporting throughout the incident management process must be maintained. Detailed records of incident investigations, actions taken, and outcomes achieved are in important part of this process. This information will be used to identify trends, measure performance, and support decision-making processes.

DEFINITIONS:

Breach of the Security of the System: Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by Clarendon College.

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.

Incident Response Team (IRT): See Security Breach Notification Policy.

Information Security Officer (ISO): Clarendon College designee who has the explicit authority and the duty to administer the information security requirements of Texas Administrative Code TAC 202.71.

Information Resources Management (IRM): The process of managing information resources to accomplish the college's missions and improve its performance, including reducing information collection burdens on the public. When standardized and controlled, these resources can be shared and reused throughout the college, not just by a single user or application.

Personal Identifiable Information (PII): Defined by statute as an individual's first name or first initial, and last name in combination with any one or more of the following data elements:

1. Social Security number;
2. Driver's license number or government issued ID number, or;
3. Health care information, such as information about an individual's physical or mental health, or;
4. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
5. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

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.

Appendix A

The following is a listing of incident categorization and prioritization ranked in order of criticality.

1. **Critical Incidents:** These are incidents that pose an immediate and severe threat to the organization's operations, data, or reputation. Examples include major data breaches, widespread malware outbreaks, or denial-of-service attacks that impact critical systems or services.

2. **High-Priority Incidents:** These are incidents that have the potential to cause significant disruption or damage if not addressed promptly. Examples include targeted phishing attacks against key personnel, ransomware infections affecting essential systems, or unauthorized access to sensitive data.

3. **Medium-Priority Incidents:** These are incidents that require attention but may not have an immediate impact on critical operations. Examples include isolated malware infections on non-essential systems, minor data leaks involving non-sensitive information, or policy violations by individual users.

4. **Low-Priority Incidents:** These are incidents that have minimal impact on operations or can be addressed without significant resources or urgency. Examples include routine software glitches, minor network interruptions, or low-risk security alerts that do not require immediate action.

5. **Incident Categories Based on Impact:** Incidents can also be categorized based on their potential impact on confidentiality, integrity, and availability of information assets. For example, incidents affecting sensitive data (such as personal information or financial records) may be prioritized higher than incidents involving non-sensitive information.

6. **Incident Categories Based on Attack Vectors:** Incidents can be categorized based on the method of attack or exploitation used by threat actors. For example, phishing attacks, malware infections, insider threats, or physical security breaches may each have their own category for prioritization and response.

7. **Regulatory Compliance Requirements:** Some incidents may need to be prioritized based on regulatory compliance requirements or legal obligations. For example, incidents involving the compromise of personally identifiable information (PII) may need to be prioritized to ensure compliance with data protection laws and regulations.

8. **Business Impact Assessment:** Conducting a business impact assessment can help prioritize incidents based on their potential impact on critical business processes, revenue generation, customer trust, or regulatory compliance. Incidents that have the greatest impact on the organization's ability to achieve its objectives may be prioritized higher for response and resolution.