Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Malicious Code Policy:

PURPOSE:
This policy is intended to provide information to College information technology resource administrators and users to improve the resistance to, detection of, and recovery from the effects of malicious code.

Clarendon College information technology resources are strategic assets that must be managed as valuable College resources. The integrity and continued operation of College information technology resources are critical to the operation of the College. Malicious code can disrupt the regular operation of College information technology resources.

The number of information technology resource 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 can reduce the risk and decrease the cost of security incidents.

SCOPE:
The Clarendon College Malicious Code Policy applies equally to all individuals utilizing Clarendon College information technology resources (e.g., employees, faculty, students, retirees, agents, consultants, contractors, volunteers, vendors, temps, etc.).

This policy does not apply to approved faculty research and academic programs where students and instructors develop and experiment with malicious programs in a controlled environment.

POLICY STATEMENT:
The following requirements shall be adhered to at all times to ensure the protection of Clarendon College information technology resources:

<u>Prevention and Detection:</u>

1. All desktops and laptops connected to the Clarendon College network must use Clarendon College-approved virus protection software and configuration.
2. Each file server attached to the Clarendon College network must utilize Clarendon College-approved virus protection software and be set up to detect and clean viruses that may infect file shares.

3. Software to safeguard against malicious code (e.g., antivirus, anti-spyware, etc.) shall be installed and functioning on susceptible information technology resources with access to the College network.
4. All information technology resource users are prohibited from intentionally developing or experimenting with malicious programs (e.g., viruses, worms, spyware, keystroke loggers, phishing software, Trojan horses, etc.) unless they are part of an approved research or academic program.
5. All information technology resource users are prohibited from knowingly propagating malicious programs, including opening attachments from unknown sources.
6. Email attachments and shared files of unknown integrity shall be scanned for malicious code before they are opened or accessed.
7. Flash drives, external hard drives, and other mass storage devices will be scanned for malicious code before accessing any data on the media.
8. Software safeguarding information technology resources against malicious code should not be disabled or bypassed by end-users.
9. The settings for software that protect information technology resources against malicious code should not be altered to reduce the software's effectiveness.
10. The automatic update frequency of software that safeguards against malicious code should not be turned off, altered, or bypassed by end-users to reduce the frequency of updates.

Response and Recovery:

1. Upon discovering a suspected malicious code, the IT department or any vendor working on behalf of the IT department must be notified as soon as possible.
2. All reasonable efforts shall be made to contain the effects of any system infected with a virus or malicious code. This may include disconnecting systems from the network or disabling service.
3. If malicious code is discovered or believed to exist, an attempt should be made to remove or quarantine the malicious code using current antivirus or other control software.
4. If malicious code cannot be automatically quarantined or removed by antivirus software, the system should be disconnected from the network to prevent further propagation of the malicious code or other harmful impact. The presence of the malicious code shall be reported to the Clarendon College IT Department.
5. Personnel responding to an incident should be given access privileges and authority to afford the necessary measures to contain/remove the infection.
6. If possible, identify the source of the infection and the type of infection to prevent recurrence.

7. Any removable media (including flash drives, external hard drives, mass storage cards, etc.) recently used on an infected machine shall be scanned before opening and/or executing any files.
8. Clarendon College-IT personnel or any vendor working on behalf of the Clarendon College IT department should thoroughly document the incident, noting the source of the malicious code (if possible), resources impacted, and damage or disruption to information technology resources, and submit to the Information Security Officer to be included in the Department of Information Resources Security Incident Reporting System.
9. Refer to the Intrusion Detection/Prevention and Security Monitory Policy for logging and recording any reported malicious code.

DEFINITIONS:
Clarendon College IT: The department or any vendor working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

Information Security Officer (ISO): Officer designated to administer the College Information Security Program.

Malicious Code: A term used to describe any code in any part of a software system or script intended to cause undesired effects, security breaches, or damage to a system.

Mitigate: The elimination or reduction of the frequency, magnitude, or severity of exposure to risks to minimize the potential impact of a threat.

Security Incident: A single event or a series of unwanted or unexpected events that involve information security (see definition of "information security event"), causing harm or threatening information assets and requiring non-routine preventative or corrective action.

Virus Protection Software: Software designed to prevent viruses, worms, and Trojan horses from getting onto a computer, as well as remove any malicious code that has already infected a computer.

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.