COMPUTER VIRUSES AND MALWARE POLICY

Eastern Oklahoma State College maintains the operational stability and efficiency of its IT systems by actively overseeing the activities and communications on the campus network and affiliated devices. This encompasses monitoring both on-campus and off-campus-originating traffic to safeguard the integrity of the College's IT infrastructure. The monitoring focuses on detecting computer viruses, malware, unauthorized system access attempts, system performance, and adherence to institutional policies. Eastern Oklahoma State College retains the authority to intercept and isolate any network traffic or computing resources that may jeopardize the security of the College's systems, data, or infrastructure. This includes, but is not limited to, files, messages, network communications, and connected devices.

Office Responsible:	Department of Information Technology
Area Information is located:	Website
Date Document was last updated:	August 15, 2023
Date Policy and Procedure was last updated:	August 15, 2023

- Every device connecting to the campus network is required to have a current and active antivirus solution installed. The antivirus software should be configured to automatically clean or quarantine any infected files as necessary. Routine automatic updates for the antivirus software are mandatory. Scheduled virus scans on devices must occur without the need for manual intervention. In cases where this automated scanning is not feasible, users hold the responsibility of initiating scans regularly and updating the software to counteract emerging threats.

- All computers issued by the College are obligated to employ the antivirus software provided and set up by the IT Services department. Modifying or disabling the installed antivirus software is prohibited unless explicitly authorized by College IT Services.

- The management of servers and network equipment for the campus is largely handled by College IT Services. Consequently, these IT Services are in charge of overseeing the antivirus systems on these systems. Interfering with, tampering, or circumventing the security and antivirus systems on equipment managed by College IT Services is a breach of the College's acceptable use policy.

- Should a computer system become infected with a virus or malicious software, actions such as blocking, quarantining, or removal from the College network may be implemented until a PC Technician or Systems Administrator confirms the system's virus-free status.

- All incoming emails directed to the College are subjected to virus, malware, and spam scans via Google. Emails posing potential risks are blocked. However, given that no security software is infallible, users must exercise prudent discretion when opening emails or attachments.

- External websites known to be sources of computer viruses and malware are prohibited and blocked. Despite this measure, users should still remain cautious when accessing external websites, as no security software can guarantee complete protection.

- In the event of a widespread virus or malware attack, College IT Services will promptly inform the College community through Broadcast emails and social media channels. Should the situation necessitate, College IT Services may initiate comprehensive system scans using the latest virus definitions. In certain cases, manual intervention may be required, and affected individuals will be directed to seek assistance at PC Support Services in the Bill Hill Library.

Additional Information

All students, faculty, and employees of Eastern Oklahoma State College must actively minimize the risk of their desktop systems infecting other systems or shared server files. Despite taking precautionary measures, the rapid spread of malicious code through means such as email and shared files can still pose a risk. Thus, maintaining up-to-date antivirus software is crucial.

- Exercise caution and never open files or macros attached to emails from unfamiliar, suspicious, or untrusted sources. Similarly, if you receive an unexpected attachment from a known individual, refrain from opening it and delete the attachment immediately.

- Dispose of spam, chain emails, and other unsolicited messages without forwarding them.

- Abstain from downloading files from sources that are unknown or seem suspicious.