ENDPOINT SECURITY STANDARD

Scope:

The Endpoint Security Standard governs the use of technologies such as desktops, laptops, and tablets owned by Kennesaw State University.

Standards and Procedures Process:

1. All computers which are the property of Kennesaw State University must have the campus-standard antivirus client installed and scheduled to perform a local scan weekly (at minimum). In addition, the anti-virus software and the virus definition files must be kept up to date.

2. KSU Antivirus Clients

Faculty/Staff/Labs

- Windows 10: Windows Defender managed by System Center
- macOS: JAMF Protect

Students

- UITS recommends using macOS XProtect and Windows 10 built-in protection. Please note that UITS staff do not formally support these packages.

3. The creation and/or distribution of malicious programs, whether intentional or not, is prohibited in accordance with USG and university policy.

4. UITS will install anti-virus software on all KSU-owned desktops and laptops.

5. It is the responsibility of end-users to install and maintain antivirus software on their personal computers and ensure that their computer is virus free.

6. Computers that are infected with malware, on which malicious traffic is detected, will be removed from the network until they are verified as “clean.”

Exceptions:

Request any exception to this standard via a service ticket to the KSU Service Desk at https://service.kennesaw.edu/

Review Schedule:

The Endpoint Security Standard will be reviewed annually by the Vice President of Information Technology and Chief Information Officer or his/her designee.

Issue Date	April 1, 2006
Effective Date	February 1, 2018
Last Updated	May 13, 2021
Responsible Office	Office of the Vice President of Information Technology and Chief Information Officer
Contact Information	Office of the Vice President of Information Technology and Chief Information Officer, Office of Cybersecurity Phone: 470-578-6620 Email: ocs@kennesaw.edu