Standard Title	Endpoint Security Standard
Issue Date	April 1, 2006
Effective Date	February 1, 2018
Last Updated	September 10, 2024
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

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:

All computers which are the property of Kennesaw State University must have the campus-standard endpoint protection client installed managed by UITS.

2. KSU Endpoint Clients

Faculty/Staff/Labs

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

Students

- UITS recommends using the built-in macOS XProtect and Windows Defender for endpoint 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 endpoint protection software on their personal devices.

6. Endpoints which demonstrate suspicious activity may be removed from the KSU network.

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.