KENNESAW STATE UNIVERSITY

Standard Title	Endpoint Security Standard
Issue Date	April 1, 2006
Effective Date	February 1, 2018
Last Updated	June 27, 2025
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:

This standard governs endpoint security requirements for devices accessing institutional data or networks at Kennesaw State University. It applies to both:

- Institutionally Owned Devices: Physical or virtual endpoints purchased, owned, or managed by KSU.
- Personally Owned Devices (BYOD): Physical or virtual endpoints owned by faculty, staff, students, or contractors that access KSU data, systems, or networks.

Applies to all Devices:

- The device is running a current, non-deprecated version of an operating system that can be updated whenever new security patches are available.
- The device operating systems and applications are regularly updated.
- The device is running antivirus and local firewall, if applicable.
- The creation or distribution of malicious software, intentional or not, is prohibited by KSU and USG policy.
- The device must not be used to circumvent institutional IT safeguards or conduct attacks on institutional IT resources. Devices exhibiting suspicious or malicious activity will be removed from the KSU network.

Additional requirements for Institutionally Owned Devices:

- All KSU-owned endpoints must have the campus-standard endpoint protection client and endpoint firewall enabled and managed by UITS.
- All KSU-owned endpoints must have full disk encryption enabled and managed by UITS, with the exception of lab and shared devices.
- The device automatically locks after 20 minutes of inactivity for Windows and MacOS endpoints (i.e., desktops, laptops, etc.).
- Access to the device is secured using the institution's central authentication (where the use of central authentication is technically possible).

Additional requirements for Personally Owned Devices (BYOD)

- The device should use strong access controls (face-ID, fingerprint, strong password,

etc).
- Ensuring university data is stored on university-provided resources
- Complying with software licensing restrictions (some applications may not be licensed for personal use).
- Collaborating with HR to ensure removal of institutional data from personal devices upon termination.

Associated Policies / Regulations

- KSU Information Technology Acceptable Usage Policy
- USG IT Handbook

Exceptions:

Endpoint devices used within the Office of Research and specialized academic purposes may not be able to accommodate some of these requirements. In these cases, risk-based accommodation will be made.

Exceptions to this standard can be requested via a service request to the KSU Service Desk at https://service.kennesaw.edu/

Review Schedule:

This standard will be reviewed annually by the Vice President of Information Technology and Chief Information Officer or designee.