Standard Title	Bring Your Own Device Standard
Issue Date	November 21, 2014
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 Kennesaw State University Bring Your Own Device Standard (BYOD) applies to all employees, consultants, and other agents who use a personally-owned device to access, store, back up, or process any institutional data.

Purpose:

The Kennesaw State University Bring Your Own Device Standard was created to align with the University System of Georgia (USG) Information Technology Handbook and mobile device best practices. Pursuant to the USG IT Handbook Section 5.1, Kennesaw State University is required to establish and maintain "appropriate academic and administrative policies, processes, and procedures to protect and secure IT infrastructure…" and the standards for end users who connect "a personally-owned device to a University System of Georgia (USG) network for business purposes".

Standard:

- Users must ensure that personally-owned devices align with the Standards defined in the USG IT Handbook Section 8.3, including (but not limited to):
  - Maintain personal device software by installing firmware, operating system and application updates promptly.
  - The use of device access protections such as biometrics, facial recognition, or passcode
  - Ensuring that confidential and/or sensitive data is protected using data encryption (built into most modern mobile devices)
  - Ensuring that data is stored on university provided resources.
  - Ensuring that confidential and/or sensitive data is not stored in cloud-based personal accounts
  - Comply with applicable policies and laws when using personally owned devices

- In partnership with Human Resources, ensuring that terminated employees "acknowledge and confirm to have all USG-sensitive data permanently erased from their personally-owned devices once their use is no longer required."
- Understanding that some software licenses do not allow installation or use on personally owned devices, and access to such software may be limited as a result, users must acknowledge that they are responsible for remaining in compliance with licensing restrictions.

Exceptions:

Exceptions to the BYOD Standard are individually reviewed by the Office of the Vice President for Information Technology and Chief Information Officer or his/her designee. The requestor must complete the following process:

- The requestor must detail the purpose of the exception and submit to the KSU Service Desk at https://service.kennesaw.edu

Review Schedule:

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