

 KENNESAW STATE UNIVERSITY	Policy Title	Data Security Policy
	Issue Date	January 1, 2011
	Effective Date	February 24, 2026
	Last Reviewed / Updated	October 9, 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

1. Policy Purpose Statement

The purpose of this policy is to provide guidance for the appropriate usage and security of confidential and sensitive information at Kennesaw State University (KSU) and is essential for compliance with federal and state law and University System of Georgia (USG) requirements.

2. Background

The KSU Data Security Policy was created to comply with the data security requirements defined in Section 12 of the *USG Business Procedures Manual*, the Section 5 of the *USG Information Technology Handbook*, the U.S. Family Educational Rights and Privacy Act (FERPA), the Payment Card Industry Standards Council (PCI), and other applicable laws, regulations, and compliance requirements.

3. Scope (Who is Affected)

The KSU Data Security Policy applies to all individuals utilizing organizational data, as defined in the *USG Business Procedures Manual*, Section 12.1 as:

Data managed in an information system by, or on behalf of, a USG organization. Organizational Data are information that record facts, statistics or information, which is read, created, collected, reported, updated, or deleted by offices of the organization. Data may be stored electronically or physically. Organizational data may reside in an organizational information system or a third-party system.

Users, hereafter referred to as data users, include, but are not limited to, students, faculty, staff, external contractors, retirees, and visitors.

4. Exclusions or Exceptions

Due to the critical importance of protecting student and employee privacy and confidentiality, the only exceptions that will be granted to the Data Security Policy concern legacy systems that are transitioning to data-at-rest encryption.

5. Definitions and Acronyms

Per the USG Business Procedures Manual, Section 12.4.2:

Confidential Information is information maintained by a USG organization that is subject to authorized restrictions on information access and disclosure, including means for protecting

personal privacy and proprietary information. (44 USC Sec 3542) Confidential classified documents are exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws.

Examples of confidential information include non-public proprietary, confidential information, and documents containing such information as Social Security number, driver's license number, state identification card number, banking account number, credit card number, debit card number, account passwords, personal identification numbers (excluding KSU IDs).

Sensitive Information is information maintained by a USG organization that requires special precautions to protect from unauthorized use, access and disclosure guarding against improper information modification, loss or destruction. Sensitive information is not exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws but is not necessarily intended for public consumption (i.e., education records and grades).

Examples of Sensitive Information include departmental continuity of operations plans, KSU ID's combined with non-confidential data elements, etc.

Unrestricted/Public Information is information maintained by a USG organization that is not exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws. Some level of control is required to prevent unauthorized modification or destruction of public information.

Examples of Unrestricted/Public Information includes KSU websites, KSU promotional materials, etc.

Cloud services: Those computing resources provided by third-party cloud service providers, who maintain and manage the underlying infrastructure, allowing users to access and utilize computing resources on-demand. Cloud services can include servers, storage, databases, networking, software, analytics, artificial intelligence models and search engines.

Additional definitions are available via the Information Technology Glossary in the [KSU Policy Portal Glossary](#).

6. Policy

- a. All data users will adhere to all current IT policies and procedures required by KSU and the Board of Regents of the University System of Georgia.
- b. Data users will only use confidential and/or sensitive information in support of the business KSU has authorized the data user to perform. Data users will not use, disclose, or publish confidential and/or sensitive information for any reason other than official KSU business.
- c. The data user understands that KSU reserves the right to legal and/or disciplinary action against the data user in the event of unauthorized use or disclosure of confidential and/or sensitive information.
- d. Confidential and/or sensitive information must not be transferred by any method to persons who are not authorized to access that information. Users must ensure that adequate security measures are in place at each destination when confidential and/or sensitive information is transferred from one location to another.
- e. Confidential information must be encrypted while at rest and while in transit, consistent with the USG *Information Technology Handbook*, Section 5.8, and State of Georgia law.
- f. Confidential and/or sensitive information must be stored and accessed in the appropriate university provided system and only copied locally if encryption or approved security

precautions have been applied to protect that information.

- g. Servers and other computers storing all university information shall have a data protection strategy in place and shall be regularly scanned for vulnerabilities and patched.
- h. While university-managed services are required for transmitting all information and records covered under FERPA, instructors may use other, non-university managed solutions to meet their pedagogical goals if (i) the information being transmitted is directory information or otherwise outside the purview of FERPA; (ii) the use of such tools is optional for students; and (iii) instructors clearly communicate the optional nature of such tools to their students. When using non-university managed tools, the instructor assumes responsibility for ensuring FERPA information is properly separated from non-FERPA information and must be able to provide evidence of such data separation in the event of an investigation or inquiry.
- i. Users are prohibited from processing, storing, or using confidential and/or sensitive information on cloud services not provided by the University.
- j. Users are required to store all institutional information in alignment with the KSU Document Management Matrix available at <https://uits.kennesaw.edu/document-management/>.

7. Associated Policies/Regulations

- a. [USG Business Procedures Manual](#)
- b. [USG Information Technology Handbook](#)
- c. State of Georgia Fair Business Practices Act ([Official Code of Georgia Annotated](#) (O.C.G.A.) § 10-1-393.8)

8. Procedures Associated with this Policy

There are no procedures associated with this policy.

9. Forms Associated with this Policy

[KSU Document Management Matrix](#)

10. Violations

- a. KSU reserves the right, at its sole discretion and without prior notice to a data user, to temporarily or permanently rescind a data user's access to confidential and/or sensitive information if it determines a breach of any provision of this policy has taken place. The data user understands and agrees that any unauthorized access or disclosure of confidential and/or sensitive information may subject the offender to disciplinary action by KSU, up to and including administrative or judicial review, termination, and/or legal action.
- b. The Office of the Vice President of Information Technology and Chief Information Officer reserves the right to disable system accounts and user accounts if activity is inconsistent with applicable laws and university policy.

11. Review Schedule

The Office of Cybersecurity will review the Data Security Policy annually.

12. Revision History

Origination Date: January 1, 2011

Revisions: October 9, 2025

For use by the KSU Institutional Policy Facilitator Only

Kennesaw State University Policy: Data Security Policy
KSU Policy Category: Information Technology

Page 4 of 4

At Kennesaw State University, institutional policies that have undergone the established shared governance review and feedback process are presented to the President and Provost for final approval. The signatures below indicate this institutional policy has been reviewed and approved by the President and Provost.

DocuSigned by:

Dr. Kathy Schwaig

11EA3F49C7FD4B9...

Dr. Kathy S. Schwaig, President
Kennesaw State University

DocuSigned by:

Dr. Ivan Pulinkala

26412C41D0DE4E2...

Dr. Ivan Pulinkala
Provost and Executive Vice President for
Academic Affairs
Kennesaw State University