Policy Title:	Data Security Policy
Issue Date:	January 1, 2011
Effective Date:	November 21, 2016
Last Reviewed:	November 18, 2016
Responsible Office:	Chief Information Officer
Contact Information:	University Information Technology Services/Information Security Office Phone: (470) 578-6620 Email: iso@kennesaw.edu

1. Purpose Statement

This policy defines the usage and security requirements of confidential and sensitive data at Kennesaw State University (KSU or the University). The purpose of this policy is to provide guidance for appropriate usage and security of confidential and sensitive information at KSU and is essential for compliance with federal, state, and University System of Georgia (USG) regulations. This policy sets forth this institution's standards with regard to the handling of confidential and sensitive institutional data and serves as the consumer data and privacy policy for the University.

2. Background

The KSU Data Security Policy was created to comply with the data security requirements defined in the U.S. Family Educational Rights and Privacy Act (FERPA), U.S. Health Insurance Portability and Accountability Act (HIPAA), USG *Information Technology Handbook*, USG Use of Encryption Policy, and USG Data Handling and Storage Policy and Standard.

3. Scope

The KSU Data Security Policy applies to all individuals utilizing University technology resources, including but not limited to students, faculty, staff, external contractors, retirees, and visitors entrusted with University data (hereafter referred to as "data user").

4. Exclusions or Exceptions

Due to the critical importance of protecting student and employee privacy, 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

Confidential Data: Confidential data includes data that the University is required to protect under the following legal or regulatory provisions:

- Family Educational Rights and Privacy Act of 1974
- Payment Card Industry Security Standards Council
- State of Georgia Personal Information (OCGA § 10-1-910-15)
- Health Insurance Portability and Accountability Act

This includes data that the University is required to protect under the following legal or regulatory provisions: Family Educational Rights and Privacy Act of 1974, Payment Card Industry Security Standards Council, Health Insurance Portability and Accountability Act, and State of Georgia Personal Information. This includes non-public proprietary or confidential information or documents containing such information as social security number, driver's license number or state identification card number, banking account number, credit card number, debit card number, account passwords or personal identification numbers (excluding KSU IDs), education records, grades.

Data User: KSU employees, external contractors, retirees, visitors, or any other authorized person who use or combine data elements in the course of their job responsibilities and/or external constituents who consume informational or data reports produced using KSU institutional data and analytics and intelligence tools. In some instances, data trustees, stewards, and managers are also data users. In other instances, KSU personnel who do not have data management responsibilities are also data users. KSU's analytic and intelligence specialists typically serve multiple roles in the data governance structure as data trustees, stewards, and managers as well as data users.

Sensitive Data: Sensitive data includes information that the university protects to reduce risk in the event of public disclosure. This includes non-public proprietary information such as, but not limited to, student email addresses, business continuity plans, infrastructure diagrams, emergency communication contacts, and public safety policies, procedures, and technical specifications.

Additional definitions are available via the IT Glossary on the KSU policy website at policy.kennesaw.edu .

6. Policy

a. The data user will adhere to all current IT policies and procedures required by KSU and the Board of Regents of the University System of Georgia.
b. The data user will only use confidential data in support of the business KSU has authorized the data user to perform. Data users will not use, disclose, or publish confidential data for any reason other than official Kennesaw State University business.
c. The data user understands that Kennesaw State University reserves the right to legal and/or dispensary action against the data user in the event of unauthorized use or disclosure of confidential data.
d. Confidential 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 data is transferred from one location to another.
e. Confidential information must be encrypted while at rest and while in transit, consistent with the USG IT Handbook 5.11 and state of Georgia Law.
f. Confidential information must not be taken off campus unless the user is authorized to do so and only if encryption or approved security precautions have been applied to protect that information.
g. Servers and other computers storing confidential information shall be regularly scanned for vulnerabilities, patched, and backed up.
h. Only University employees who have written authorization from the relevant data steward(s) may have access to confidential data.

7. Associated Policies/Regulations

a. USG *Information Technology Handbook*, Section 5.11 Minimum Security Standards for USG Networked Devices
b. USG *Information Technology Handbook*, Section 9.5 Privacy and Security
c. State of Georgia Fair Business Practices Act (OCGA §10-1-393.8)

8. Procedures Associated with this Policy

a. This policy has no associated procedures.

9. Forms Associated with this Policy

a. This policy has no associated forms.

10. Violations

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 information if the University 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 information may subject the offender to disciplinary action by KSU, up to and including administrative or judicial review, termination, and/or legal action.

11. Review Schedule

The KSU Data Security Policy is reviewed annually by the Office of the CIO or his/her designee.