Policy Title	Enterprise Information Security Policy
Issue Date:	September 1, 2006
Effective Date:	November 21, 2016
Last Reviewed:	November 18, 2016
Responsible Office:	Chief Information Officer
Contact Information:	Information Technology Services/ Information Security Office Phone: (470) 578-6620 Email: iso@kennesaw.edu

1. Purpose Statement

This policy serves to establish the minimum information security practices for Kennesaw State University technology resources, devices, and associated communication. This policy is intended to provide direction on University security practices designed to ensure the confidentiality, integrity, and availability of University information.

2. Background

The Kennesaw State University Enterprise Information Security Policy was created to comply with the University System of Georgia (USG) *Information Technology Handbook*. Pursuant to the USG *Information Technology Handbook*, Kennesaw State University (KSU or the university) "must provide for the integrity and security of its information assets by creating appropriate internal policies, processes, standards, and procedures for preserving the integrity and security of each automated, paper file, or database."[1]

3. Scope

The KSU Enterprise Information Security Policy applies to all individuals utilizing University technology resources, including but not limited to students, faculty, staff, external contractors, retirees, and visitors. Additionally, any remote access (e.g., ISP access, VPN connection, etc.) onto the KSU enterprise network or associated domains will have the same effect as direct access via KSU-provided equipment or

[1] USG Information Technology Handbook 5.1.2, Policy, Standards, Processes, and Procedure Management Standard, http://www.usg.edu/information_technology_services/it_handbook/

facilities.

4. Exclusions or Exceptions

Individuals may be exempted from this policy only upon written approval of the Chief Information Officer.

5. Definitions

Definitions are available via the Information Technology (IT) Glossary associated with this policy on the Policy at KSU website (policy.kennesaw.edu).

6. Policy

Information security is defined as the protection of information and its critical elements, including the systems and hardware that store, use or process, and transmit that information. The KSU Information Security Office is responsible for architecting and implementing the KSU Information Security Program, as required in the USG *Information Technology Handbook*. Kennesaw State University's information security model is based on the ISO 27001 framework and utilizes technical, operational and managerial safeguards to mitigate university risks. These safeguards, along with others, act collectively to ensure data availability, confidentiality, and integrity at KSU. As is required by the USG *Information Technology Handbook*, KSU submits annual status reports to the USG regarding the status of the institution's information security program.

Protection of University information assets and the technology resources that support the enterprise is critical to the functioning of the University. University information assets are at risk from potential threats such as employee error, malicious or criminal action, system failure, and natural disasters. Such events could result in damage to information resources, corruption or loss of data integrity, or the compromise of data confidentiality. The University's Information Security Office seeks to proactively reduce the risks to electronic information resources through the implementation of controls designed to detect and prevent errors before they occur. Detrimental access to the KSU enterprise network is defined as any intervention, from either an internal or external entity, that creates any situation whereby authentication and access control mechanisms are bypassed that may compromise the confidentiality, integrity, or availability of information resources.

KSU technology resources proactively track detrimental access activity and work to prohibit or correct such activity. Where unintentional detrimental access activity is detected, the affected organization will be advised to correct exploitable vulnerabilities to prevent future occurrences. Where detrimental access activity is determined to be intentional, it will be assumed to be malicious and an appropriate response will be initiated.

KSU reserves the right to examine all information transmitted through the university's enterprise network. University IT resources should be used for appropriate academic and business purposes only. Examination of information stored or transmitted on university IT systems may take place without prior warning to the parties sending or receiving such information.

In addition, most files and documents maintained by KSU are subject to public review under the Georgia Open Records Act. This includes computer files and other data, regardless of the medium of storage. Although all members of the university have an expectation of privacy, if a user is suspected of violating policy, his or her right to privacy may be superseded by the university's requirement to protect the integrity of IT resources, the rights of all users, and the property of KSU and the state of Georgia. KSU thus reserves the right to examine material stored on or transmitted through its resources if there is cause to believe that the standards for appropriate use are being violated.

7. Associated Policies/Regulations

a. The Georgia Computer Systems Protection Act (OCGA § 16-9-93)
b. USG *Information Technology Handbook*, 5.1 Information Security Program

8. Procedures Associated with this Policy

a. As required by information in Section 7.

9. Forms Associated with this Policy.

a. As required by information in Sections 7 and 8.

10. Violations

All data processed, stored, and transmitted over KSU networks and machines is held in great trust and must be afforded the greatest safeguards. To this end, information security policy, education, processes, and standards created to protect KSU information assets rely upon the Georgia Computer Systems Protection Act (O.C.G.A 16-9-90 through O.C.G.A. 16-9-94) to ensure compliance. Violators will be prosecuted accordingly.

11. Review Schedule

The Enterprise Information Security policy is reviewed annually by the Office of the CIO and the KSU Chief Information Security Officer.