



# **Enterprise Information Security Policy - EISP**

## **Office of the Vice President for Information Technology / CIO**

---

---

### **PURPOSE:**

This policy serves to establish minimum information security practices for Kennesaw State University computer resources and associated communication networks utilizing the Kennesaw State University enterprise network.

Furthermore, this policy is intended to give direction on University security practices designed to ensure the confidentiality, integrity, and availability of campus data. This document also specifies the review and revision schedule of the policy.

### **INFORMATION SECURITY ELEMENTS:**

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. Kennesaw State University uses a layered security model consisting of technical controls, education & awareness, and policy designed to ensure data confidentiality, integrity, and availability. This policy is intended to give direction on accepted security practices.

## **POLICY STATEMENT:**

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 compromise to data confidentiality. The University Information Security Office policies and guidelines seek to reduce the risks to electronic information resources through implementation of controls designed to detect and prevent errors that may occur. Detrimental access to the Kennesaw State University 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 or integrity of information resources or render it unavailable. Kennesaw State University technology resources will 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 as malicious activity and an appropriate response will be initiated.

## **INFORMATION TECHNOLOGY STANDARDS AND GUIDELINES:**

Revised: 09/01/2006  
NIST Framework: Policy

The Georgia Computer Systems Protection Act (O.C.G.A. 16-9-90) specifies unlawful acts involving information resources and subsequent penalties upon conviction. All data processing, residing or transiting Kennesaw State University networks and machines is held in great trust and it must be afforded the greatest safeguards. Therefore, information security policy, instruction, processes, and standards created in furtherance of protecting Kennesaw State University information assets rely upon the Georgia computer Systems Protection Act (O.C.G.A 16-9-90) to ensure compliance. Violators will be prosecuted accordingly.

### **APPLICABILITY:**

All Kennesaw State University faculty, staff, students, contractors, agents or other individuals utilizing computer resources, data communication networks, or other information technology infrastructure resources owned or leased by Kennesaw State University; including any other state agencies having electrical connectivity to the network are subject to this policy. Additionally, any remote access such as dial up connections, ISP access, VPN connection onto the Kennesaw State University enterprise network or associated domains will have the same effect as direct access via KSU provided equipment or facilities.

### **NEED FOR INFORMATION TECHNOLOGY SECURITY:**

All data and information sent over the Kennesaw State University enterprise network, and associated domain communications systems, are the property of

Revised: 09/01/2006  
NIST Framework: Policy

Kennesaw State University. In order to maintain and manage this property, Kennesaw State University reserves the right to examine all information transmitted through these systems. Kennesaw State University computer and communications systems should be used for appropriate academic and business purposes only. Examination of such information may take place without prior warning to the parties sending or receiving such information.

In addition, most files and documents maintained by Kennesaw State University are subject to public review under the Georgia Open Records Act. This includes computer files and other data regardless of the medium of storage. For these reasons faculty, staff, students, contractors, agents or other individuals should have no expectation of privacy associated with the information they store in or send through these systems. These systems exist to support mission critical University activities and goals.

### **REVIEW SCHEDULE:**

The Enterprise Information Security policy will be reviewed annually by the Office of the Vice President for Information Technology & Information Security Officer.

### **AUTHORITY:**

Authority to establish and enforce this policy and associated security policy documents is made by Chief Information Officer and Information Security Officer.