Network Access Policy

Office of the Vice President for Operations/CIO

**Purpose:**

This document sets forth the policy regarding the use of Kennesaw State University’s wireless and wired network access. The purpose of this policy is to provide guidance for appropriate usage of wireless and wired resources available to the KSU community. This policy supports the free and open exchange of information and the provision of technology to advance the educational purposes for the University’s students, faculty and staff, while also taking data confidentiality and integrity into account.

In support of the KSU mission, Information Technology Services will be the sole provider of network resources for the entire KSU community with the exception of student housing.

**Definitions:**

Definitions are available via the IT Glossary on the ITS Information Security Office website.

**Scope:**

Kennesaw State University is committed to providing a secure network that protects the integrity and confidentiality of information while maintaining accessibility. This policy is designed to apply to all currently employed faculty, staff, and currently enrolled students. It also applies to other individuals using the campus network such as, but not limited to, alumni, visitors, visiting faculty, temporary staff members, and contractors.

**Issue Date:**

This University Network Access Policy was issued on January 1, 2004

**Effective Date:**

Revised: 09/13/2010
ISO Domain: Policy
This policy is effective as of January 1, 2011

**Policy:**

**Responsibilities of User(s)**

It is the responsibility of the users to ensure that Wireless and Wired access is used in a fair and responsible manner.

- Users should keep their NetIDs and passwords confidential.
- All network users shall abide by this policy and all applicable Policies and Procedures, or risk loss of access privileges and referral to the proper campus authorities for potential action.
- While wireless connectivity is appropriate for web surfing or email access, wireless users share bandwidth and, as number of users increase, the available bandwidth per user diminishes. If a user needs to download presentations or any other application for their academic usage it is recommended to connect through wired ports.

**Responsibilities of Departments**

- University employees and students may not install wireless access points or other equipment on the University network. If a wireless access point is found on the KSU network which is installed without prior approval from ITS, it will be considered a Rogue access point and service to this device may be discontinued.
- University standards require that wireless access points have security and authentication built into them to ensure that unauthorized persons will not be able to gain access to the University network. Service to devices which fail to meet this standard may be discontinued.
- Other devices using the same radio frequencies as wireless access points may interfere with the KSU Enterprise Wireless Network. If such a device is installed without prior approval from ITS, it will be considered a Rogue access point and service to this device may be discontinued.
- If a faculty/staff member notices any abuse or misuse regarding KSU network access they should immediately report it the KSU Service Desk.
- In case of interference or disruption with wireless or wired connectivity, department personnel should report it to the KSU Service Desk.
Responsibilities of ITS

- The Information Technology Services is the sole provider of the deployment and management of University Networks. ITS handles all issues regarding access, connectivity, and interference of KSU Network. Whenever possible, network issues will be diagnosed and resolved in a timeframe which causes the least amount of impact to the campus. KSU network users will be notified of such outages by the ITS Help Desk.

Authorized Access and Usage of Network Resources:

Authorized access to the network is a privilege and not a right. Any person officially affiliated with the university, with a valid Network ID (NetID), can access the KSU Network.

Systems that are the property of KSU will be granted a level of network access that is controlled by a centralized Identity Management System. All other systems brought on campus by faculty, staff, or students will be identified by the network and potentially placed into a controlled, monitored network.

Bandwidth and port access may be limited to systems based on the users’ affiliation with the university. Access to services through public access labs is restricted to current employees or students. Termination or suspension will automatically revoke these privileges.

ITS reserves the right to guarantee bandwidth for mission critical services, change the available bandwidth per user based on usage, and reduce or deny internet service to users that violate university IT Policies.

Exceptions:

Exceptions to the University Network Access Policy are individually reviewed by the Director of Information Technology Services and must follow the following process:

- If faculty/staff members want to design special academic networks (not connected to the KSU network), in pursuit of their educational or research mission, the faculty must request approval and collaborate with ITS to ensure that the KSU network is not adversely affected by the equipment or services of the academic network.
- In order to effectively evaluate the request and evaluate existing technology usage, requests for exceptions should detail the purpose of the request and how the KSU enterprise network is insufficient to address the need.
Please submit requests to netadmin@kennesaw.edu with a carbon copy to iso@kennesaw.edu.

Policy Violations:

If an employee or student witnesses any violation of policy they should report it directly to ITS via abuse@kennesaw.edu. If any employee or student witnesses a criminal act, they should notify KSU Public Safety. Information Technology Services expects fair and responsible usage of KSU Network resources. In the case of KSU Network abuse, the rights of the users can be suspended.

Individuals using KSU Network resources are prohibited from use of the system to commit a criminal act. This includes (but not limited to) unauthorized access or attempt to access other systems, the implementation of any virus or malicious program, downloading and/or distribution of music, movies, or any other electronic media in which legal copyright is not owned, or any use of the system to plan, commit, or exploit criminal activities.

Individuals in violation of this policy are subject to a range of sanctions including, but not limited to, the loss of computer or network access privileges, disciplinary action, dismissal from the University, and/or legal action. Some violations may constitute criminal offenses, as outlined in the Georgia Computer Systems Protection Act and other local, state, and federal laws.

External Documents and Links:

- Perimeter Firewall Standard

Review Schedule:

The KSU Computer Usage Policy will be reviewed annually by the Office of the Vice President for Operations/CIO or their designee.