

# KSU Network Access Policy



## Office of the Vice President for Information Technology

### 1. Statement of Policy

This document sets forth the policies for Kennesaw State University's wireless and wired network access. The purpose of this policy is to provide guidance for the implementation of appropriate usage for wireless and wired connectivity for KSU community. Thus incorporating the mission of the Kennesaw state University to flourish campus community through the free and open exchange of information, provide technology to advance educational purposes and meet the needs of students, faculty and staff.

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.

#### 1.1. *Scope and Applicability*

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 any individual enjoying the privileges and rights of the university as a visitor, visiting faculty, or temporary staff member.

#### 1.2. *Definition of Technology Addressed*

**KSU Network Access**- KSU Network Access includes the backbone network and all Local Area and Wireless Networks at the Kennesaw State University.

**Client Systems (hardware/software)** – Client systems include any equipment and software that is installed on a desktop, laptop, handheld-, portable-, or other computing device.

**Wireless Zone** – Wireless zone accommodates wireless devices in the internal Campus Zone. It allows users to connect directly to the internal KSU network without using VPN access. Wireless infrastructure includes wireless access

points, antennas, cabling, power, and network hardware associated with the deployment of a wireless communications network.

**Network Access ID (NetID)** – This is the identification key used to authenticate a user and provide access to their resources.

**Pre-Shared key** – This is a common key that will network users will need in order to use wireless service.

**SSID** – A Service Set Identifier is a name that identifies a wireless network. All devices on a specific wireless network must know its SSID.

**User Authentication** - A method verifying that the user of a wireless system is a legitimate user, independent of the computer or operating system being employed.

**Wireless Access Point** – Wireless access point is any piece of equipment that allows wireless communication using transmitters and receivers. These devices act as hubs and allow communications to the campus network.

**WiFi Protected Access** – This is a system used to encrypt and decrypt data signals transmitted between Wireless LAN devices.

**Interference** - Interference is the degradation of a wireless communication signal caused by electromagnetic radiation from another source. Such interference can either slow down a wireless transmission or completely eliminate it depending on the strength of the signal.

**Privacy** - Privacy is the condition that is achieved when successfully maintaining the confidentiality of personal, student and/or employee information transmitted over a wireless network.

**Security** - Security, as used in this policy, not only includes measures to protect electronic communication resources from unauthorized access, but also includes the preservation of resource availability and integrity.

**ICS Scanning** – This is the end point scan to ensure that client systems are not infected with malicious software.

### **1.3. Responsibilities**

#### **1.3.1 Responsibilities of Users**

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 the KSU Acceptable Use Policy or risk loss of network privileges and referral to the proper campus authorities for further action.

- Wireless connectivity is appropriate for web surfing or email access, wireless users share bandwidth, as number of users increase the available bandwidth per user diminishes, therefore, if a user needs to download presentations or any other application for their academic usage they should connect through wired ports.

### **1.3.2 Responsibilities of Departments**

- If a faculty members want to design special academic networks, not connected to the KSU network, in pursuit of their educational or research mission, the faculty must involve ITS in the design to be sure that the KSU network is not adversely affected by the equipment or services of the academic network.
- If a faculty/staff member notices any abuse or misuse regarding KSU network access they should immediately report it to ITS.
- In case of interference or disruption with wireless or wired connectivity, department personnel should report it to ITS.

### **1.3.3 Responsibilities of ITS**

The Information Technology Services is the sole provider of the deployment and management of the KSU Networks. ITS handles any issues regarding access, connectivity, and interference of the KSU Network Access. ITS will inform KUS network users about security, privacy policies and procedures related to the KSU Network accessibility.

## **2. Authorize 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 and has a valid Network ID (NetID) can access 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 placed into a controlled, monitored network.

Bandwidth and port access may be limited to systems based on the users' affiliation with the university. Possible affiliations are: Faculty, Staff, Student (Alumni), Guest, Unregistered.

Access to services through public access labs is restricted to current employees or students. Termination or suspension will automatically revoke these privileges.

## **2.1. Disruptive use or misuse**

Information Technology Services expects a fair and responsible usage of KSU Network access from its users. However, in case of misuse of the KSU Network, the rights of the users can be suspended.

## **2.2. Criminal use**

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 virus-type program, or any use of the system to plan commit or exploit criminal activities.

## **3. Systems Management**

Please refer to the Computer Usage policy

## **4. Violations of Policy**

This policy is legally binding to all faculty, staff and students currently employees or enrolled at Kennesaw State University or other individuals who used KSU Network Access. If any employee or student witnesses any violation of policy they should notify their head or report it directly to the ITS. If any employee or student witnesses a criminal act, they should notify campus security.

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; the University will carry out its responsibility to report such violations to the appropriate authorities.

For the first or minor violation of this policy, the incident may be dealt with at the ITS or appropriate administrative unit level. The alleged offender will be furnished a copy of the Network Access Policy and University Computer and Network Usage Policy and will sign a form agreeing to conform to the policy. All incidents and consequences must be reported to Information Technology Services.

Subsequent or major violations of these policies will be reported to Information Technology Services who may then forward a report to either the Vice President for Student Success and Enrollment Services (for students) or the appropriate judicial channels (for employees) for the determination of sanctions to be imposed.

## **5. Policy Review and Modification**

The KSU Computer Usage Policy will be reviewed annually by the Office of the Vice President for Information Technology

## **6. Limitations of Liability**

Kennesaw State University will make no effort to support individuals found guilty of policy or criminal violations. University policy expressly prohibits providing legal defense to anyone suspected or charged with criminal policy involving university property. Any individual accused of misconduct or criminal behavior via the use of KSU Network resources will receive no legal protection. IF convicted of any violations, the university reserves the rights to impose liability for the consequences of such acts and seek indemnification from the guilty party for damages the university may incur, if appropriate.

I have read and understand the above policy and will comply with its provisions. I understand that failure to comply with the terms of this document will result in denial of access to KSU Networks.