Policy Title:	Network Access Policy
Issue Date:	January 1, 2004
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 covers the use of Kennesaw State University's wireless and wired network access and provides guidance for appropriate usage of wireless and wired resources available to the Kennesaw State University (KSU or the University) community. This policy supports the free and open exchange of information and the provision of technology to advance the educational mission of the University while also protecting data confidentiality and integrity.

In support of the KSU mission, University Information Technology Services (UITS) is the sole provider of network resources for the KSU community, with the exception of student housing.

2. Background

The Kennesaw State University Network Access Policy was created to comply with the University System of Georgia (USG) information technology policies. Pursuant to the USG *Information Technology Handbook*, Section 5.1.2, KSU is required to establish and maintain "appropriate internal policies, processes, standards, and procedures for preserving the integrity and security of each automated, paper file, or database."

3. Scope

UITS is committed to providing a secure network that protects the integrity and confidentiality of information while maintaining accessibility. The KSU Network Access Policy applies to all currently employed faculty, currently employed staff, and currently enrolled students as well as to other individuals using the campus network, including but not limited to alumni, visitors, visiting faculty, temporary staff members,

and contractors.

4. Exclusions or Exceptions

Exceptions to the University Network Access Policy are individually reviewed by the Associate Chief Information Officer and Associate Vice President of Information Technology and must follow the following process:

- If faculty or staff want to design special academic networks (not connected to the KSU network) in pursuit of their educational or research mission, the faculty or staff must request approval and collaborate with UITS 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.
- Requests for special academic networks must be submitted to netadmin@kennesaw.edu with a carbon copy (cc:) to iso@kennesaw.edu.

5. Definitions

Definitions are available via the IT Glossary on the KSU Policy Portal at policy.kennesaw.edu.

6. Policy

a. 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.

1) Users should keep their NetIDs (network identification) confidential.
2) Users must keep their password confidential.
3) 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.
4) While wireless connectivity is appropriate for Web surfing or email access, wireless users share bandwidth and, as the number of users increase, the available bandwidth per user diminishes. If a user needs to download presentations or any other application for academic usage, the user is encouraged to connect through wired ports.

b. Responsibilities of Departments

1) 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 that is installed without prior approval from UITS, it will be considered a rogue access point and service to this device

may be discontinued.

2) 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. Devices which fail to meet this standard may be disconnected.

3) 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 UITS, it will be considered a rogue access point and service to this device may be discontinued.

4) Faculty/staff who notice any abuse or misuse regarding KSU network access, should immediately report it to the KSU Service Desk.

5) Department personnel should report interference or disruption with wireless or wired connectivity to the KSU Service Desk.

c. Responsibilities of University Information Technology Services (UITS)

University Information Technology Services (UITS) is the sole provider of the deployment and management of the University network. UITS handles all issues regarding access, connectivity, and interference of the KSU network. Whenever possible, network issues will be diagnosed and resolved in a timeframe that causes the least impact to the campus. KSU network users will be notified of such outages by the KSU Service Desk.

d. USG Minimum Standards

1) The University System of Georgia Minimum Standards for the Security of University System of Georgia Networked Devices requires that passwords used for authentication of networked devices meet the USG Strong Password Standard. These requirements are stated below.
   i. Are at least 10 characters in length.
   ii. Must contain characters from at least three of the following four types of characters:
      a) English upper case (A-Z);
      b) English lower case (a-z);
      c) Numbers (0-9);
      d) Non-alpha special characters ($, !, %, ^, …).
   iii. Must not contain the user's name or part of the user's name.
   iv. Must not contain easily accessible or guessable personal information about the user or user's family.

e. Authorized Access and Usage of Network Resources

1) Authorized access to the network is a privilege, not a right. Any person officially affiliated with the University who has a valid Network ID (NetID) can access the KSU network.
2) 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.
3) 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 and students. Termination or suspension will automatically revoke these privileges.
4) UITS 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 who violate University IT Policies.

7. Associated Policies/Regulations

a. USG *Information Technology Handbook,* 5.11: Minimum Standards for the Security of University System of Georgia Networked Devices
b. USG *Information Technology Handbook,* 5.12.3: Password Security and Composition Standard

8. Procedures Associated with this Policy

a. Perimeter Firewall Standard
b. Bring Your Own Device Standard

9. Forms Associated with this Policy

a. As applicable in Sections 7 and 8 above.

10. Violations

Anyone who witnesses a violation of policy should report it directly to UITS via abuse@kennesaw.edu. Anyone who witnesses a criminal act should notify KSU Public Safety. University 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 by the University.

Individuals using KSU network resources are prohibited from using the system to

commit a criminal act. This includes, but is not limited to, unauthorized access or attempt to access other systems; the implementation of any virus or malicious program; downloading and/or distributing music, movies, or any other electronic media in which legal copyright is not owned; or any use of the system to plan or commit 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 or termination by the University, and/or other legal action. Some violations may constitute criminal offenses as outlined in the Georgia Computer Systems Protection Act and other local, state, and federal laws.

11. Review Schedule

The Network Access Policy is reviewed annually by the Office of the CIO or his/her designee.