Policy Title:	New Server Policy
Issue Date:	February 1, 2007
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

Servers at Kennesaw State University (KSU or the University) play an important role in the delivery of critical data to students, faculty, staff, and the public. To this end, safeguards must be in place to protect the confidentiality, integrity, and availability of the data housed on these servers. Technical, managerial, and operational safeguards work together to assure that new servers are installed and configured in such a manner to emphasize security and minimize service disruptions. These requirements are outlined in this policy and collectively define the University's required server base configuration.

2. Background

The Kennesaw State University New Server 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

The KSU New Server Policy applies to all class A, B, or C servers hosted at/by KSU as defined in the IT Policy Glossary.

4. Exclusions or Exceptions

Servers isolated to departmental private networks which do not require firewall rules or University DNS records are exempt from this policy. Servers that process,

transmit, or store KSU confidential data may be exempted only with the approval of the Chief Information Officer (CIO).

5. Definitions

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

6. Policy

All servers connected to the KSU network after May 1, 2007 must meet the applicable hardening requirements outlined in the KSU New Server Configuration Standard. Servers that process, transmit, or store KSU confidential data must satisfy additional requirements outlined in the document.

Once a new server has been configured to meet the University-required hardening standards, the primary administrator must complete the New Server form available via the UITS Application Portal at http://apps.kennesaw.edu (KSU NetID authentication is required to access the site).

Prior to a new server entering production status, a security scan of the system must be completed by the Information Security Office. Identified risks must be communicated to the system administrator and must be corrected or justified. Requests for scans should be directed to iso@kennesaw.edu.

The system administrator must attend monthly KSU System Administrator meetings. If unable to attend, the administrator may send a representative in his/her stead.

Remote administration of KSU servers must be routed through the campus Virtual Private Network (VPN). VPN access can be requested through the University Information Technology Services (UITS) Service Desk at: service@kennesaw.edu.

7. Associated Policies/Regulations

a. None.

8. Procedures Associated with this Policy

a. Server Configuration Standard
b. Server Auditing Standard

9. Forms Associated with this Policy

a. As applicable in Section 8 above.

10. Violations

Any servers connected to the KSU network after May 1, 2007 that are found to be in violation of the KSU New Server Policy may be disconnected from the network without notice and employees may be subject to disciplinary action.

11. Review Schedule

The New Server Policy is reviewed annually by the Office of the Chief Information Officer or his/her designee.