Server Configuration Standard

**Issue Date:**

The Server Configuration Standard was issued on June 1, 2007

**Effective Date:**

The Server Configuration Standard is effective as of November 29, 2016

**Standard:**

Applicable to all new servers:

- A server must not be connected to the KSU network until it meets all of the applicable requirements outlined herein, and a New Server form has been completed for the server. Limited connectivity, via DHCP addressing, is allowed for patching purposes only.
- The operating system must be installed from a legal licensed copy.
- Server must have a primary administrator documented on the server’s New Server Form.
- Server must have the most recent vendor supplied patches installed (unless there is a known compatibility issue), and must be monitored for updates weekly.
- All unnecessary services, software, and drivers must be removed or disabled.
- All default accounts must be renamed and/or their password changed.
- System and service logging must be enabled, and the logs audited for suspicious activity weekly. Auditable events include, (but are not limited to), user logon/logoff, confidential file(s) copy/move/delete/create/modify, web server activity logs, and database transaction logs.
- Logs must be maintained a minimum of 30 days.
- All Windows-based servers must have an AntiVirus product installed which is updated weekly (unless there is a service interruption issue).
- Accounts must only be given the level of access needed.
- All DNS record updates must be submitted via the KSU Server Request Form at apps.kennesaw.edu
• Server & service downtime must be scheduled with affected users whenever possible. Please notify the UITS Service Desk at service@kennesaw.edu in the event of extended downtime.
• FTP & Telnet hosting is forbidden, inquiries regarding this type of hosting can be directed towards the KSU Information Security Office, available via iso@kennesaw.edu
• DNS hosting requires permission from the KSU Networking Group, available via http://apps.kennesaw.edu

Additional Requirements for Class-A Servers:

• Server must be connected to an uninterruptible power supply (UPS) which is maintained for battery life & runtime regularly.
• Server must be in a room which is secured in such a way to allow auditing of individuals entering the room.

External Documents and References:

• Windows Server Security Best Practices
• OS X Server Security Best Practices
• Linux Server Security Best Practices

Current versions of these documents are available via the UITS-ISO website at http://uits.kennesaw.edu/infosec/

Review Schedule:

The New Server Configuration Guidelines will be reviewed annually by the Office of CIO or their designee.