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 February 1, 2018

Standard:

Applicable to all new servers:

- A server must not enter a production state until it meets all of the applicable requirements outlined herein, and a new server request has been submitted to the KSU Service Desk at service@kennesaw.edu.
- Primary system administrator must be indicated on the request service ticket. A technician from the Office of CIO’s Office of Cybersecurity will contact the primary system administrator to discuss requested services, anticipated data sets, and associated business processes.
- The operating system must be installed from a legal licensed copy.
- Server must have the most recent vendor supplied patches installed (unless there is a documented compatibility issue), and must be monitored for updates weekly.
- All unnecessary services and software 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 reviewed 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 in alignment with the KSU Server Auditing Standard.
- All Windows-based servers must have an endpoint security product installed which is updated weekly (unless there is a service interruption issue).
• Accounts must follow the principle of least privilege.
• All DNS record updates and DNS hosting requests must be submitted via KSU Service Desk at service@kennesaw.edu.
• Server & service downtime must be scheduled with impacted users whenever possible. Please notify the Office of the CIO’s Service Desk at service@kennesaw.edu in the event of extended downtime.
• FTP & Telnet hosting is forbidden. Inquiries regarding this type of hosting should be directed to the KSU Service Desk at service@kennesaw.edu.

Additional Requirements for Class-A & B Servers:

• Server must be in an Office of the CIO data center which is connected to an uninterruptible power supply (UPS) and maintained for battery life and runtime regularly.
• Server must be in an Office of the CIO data center 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 Office of the CIO’s OCS website at http://uits.kennesaw.edu/infosec/

Review Schedule:

The New Server Configuration Guidelines will be reviewed annually by the Office of Chief Information Officer and Vice President for Information Technology or his/her designee.