



SERVER CONFIGURATION STANDARD

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 <https://service.kennesaw.edu>
- The System administrator must be indicated on the request service ticket. A member of the UITS Office of Cybersecurity will contact the system administrator to schedule a vulnerability management scan, share findings and remediations and certify the server as production.
- The operating system must be installed from a legal licensed copy.
- Server must be included in a regular change management process, ensuring that the most recent vendor supplied patches are installed in a timely manner.
- Server software and services should be appropriately minimized
- Accounts must follow the principle of least privilege.
- All default account passwords must be changed.
- As applicable, default accounts must be renamed.
- 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 file servers must have an endpoint security product installed which is updated regularly.
- All DNS record updates and DNS hosting requests must be submitted via the KSU Service Desk at <https://service.kennesaw.edu>.
- Server & service downtime must be scheduled with impacted users whenever possible. Please notify the UITS Service Desk at <https://service.kennesaw.edu> in the event of extended downtime.
- Effective June 30, 2020 all servers must only be remotely manageable via VPN with Multifactor Authentication.
- FTP & Telnet hosting is restricted. Inquiries regarding this type of hosting should be directed to the KSU Service Desk at <https://service.kennesaw.edu>

Additional Requirements for Class-A & B Servers*:

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

* Server classifications, including Class A and Class B, are available via the ***KSU Policy Resources*** link on <https://policy.kennesaw.edu>

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 OCS website at <http://uits.kennesaw.edu/infosec/>

Review Schedule:

The New Server Configuration Guidelines will be reviewed annually by the Office of the Chief Information Officer (CIO) and Vice President of Information Technology or their designee.

| | |
|---------------------|--|
| Issue Date | April 1, 2006 |
| Effective Date | February 1, 2018 |
| Last Updated | May 13, 2021 |
| Responsible Office | Office of the Vice President of Information Technology and Chief Information Officer |
| Contact Information | Office of the Vice President of Information Technology and Chief Information Officer, Office of Cybersecurity Phone: 470-578-6620 Email: ocs@kennesaw.edu |