Server Auditing Standard

Issue Date:
The Server Auditing Standard was issued on February 8, 2010

Effective Date:
The Server Auditing Standard is effective as of November 29, 2016

Scope:
These requirements apply to all class A, B, or C servers hosted at Kennesaw State University, as defined in the IT Policy Glossary. Network infrastructure devices (switches, routers, etc), network printers, relational database management systems, and web content management systems are excluded from these requirements.

Purpose:
To establish uniform auditing standards across KSU's IT systems, increase accountability, and aid with preserving data integrity. These logging standards will help mitigate potential risks, facilitate incident responses in the event of a compromise, and align with State of Georgia Audit requirements.

Standard:
Retention: Logs should be retained for a minimum of 30 days. For systems in which log volume makes 30-day retention unfeasible, logs should be retained as long as possible without affecting the availability of hosted services.

All Servers
- Account creations / deletions
- Password resets
- Service installation / removal
- Restarts / shutdowns
- Patching
- Configuration changes
Web Servers *(in addition to “All Servers” section)*
- Access to confidential data as defined by the Georgia Personal Identity Protection Act
- Page updates & deletions (SFTP, FTP, SSH, HTTP, HTTPS)

Mail Transfer Authority *(in addition to “All Servers” section)*
- Administrator logins
- Configuration changes

**Review Schedule:**

The Server Auditing Standard will be reviewed annually by the CIO or their designee.