Perimeter Firewall Standard

**Issue Date:** The Perimeter Firewall Standard was issued on January 15, 2009

**Effective Date:** November 29, 2016

**Purpose:**

The Kennesaw State University Perimeter Firewall facilitates network security at the campus gateway and segregates traffic security for the campus network. The Perimeter Firewall Standard defines the responsibilities for KSU’s perimeter firewall administration, thus ensuring that services offered off campus are provided in a secure manner and that legacy exceptions are removed when applicable.

**Standard:**

The perimeter firewall permits the following outbound and inbound network traffic:

- **Outbound** – Allow all internet traffic to hosts and services outside of the campus with the exception of known security vulnerabilities, servers that generate email messages with a non-campus destination, or other exceptions.
- **Inbound** – Users may only access defined services that support the university mission. These services must be communicated to the campus firewall administrator, via secure web form, and reviewed before inclusion.

**Default to Deny All**

Every Internet connectivity path and service not specifically permitted by this policy, or documented via the UITS server form, will be blocked by the Kennesaw State University Firewall. The current firewall rule base is documented by UITS Networking and available to all KSU systems administrators. New firewall rule
requests will be reviewed by staff from the UITS Networking team and evaluated on 2 factors:
- The request is supports the mission of the University
- Security controls have been employed as applicable
Requests which fail to meet these 2 requirements will be brought to the attention of the UITS Executive Director - Networking and the KSU Information Security Officer for further review.

Firewall Dedicated Functionality
Any firewall used to protect KSU’s internal data networks must run on a dedicated device. These devices may not serve other purposes including, but not limited to, acting as web or email servers.

Firewall Change Control
Firewall configuration rules and permissible service rules are created upon request and approval from both UITS Networking and Security & Information Security Office. Requests for new rules will be processed within 24 hours or submission.

Regular Auditing
Because firewalls provide such an important barrier to unauthorized access to KSU networks, they must be audited on a regular basis. At a minimum, this audit process must include consideration of defined configuration parameters, enabled services, permitted connectivity, current administrative practices, and adequacy of the deployed security measures. The audits must be performed by technically proficient persons other than those responsible for the administration of the firewall.

Logs
All changes to firewall configuration parameters, enabled services, and permitted connectivity must be logged. In addition, all suspicious activity which might be an indication of unauthorized usage or an attempt to compromise security measures must also be logged. These logs must be promptly removed from the recording systems and stored in a physically protected container for at least 30 days after the time they were recorded. These logs must be reviewed periodically to ensure that the firewalls are operating in a secure manner.

Physical Security
All KSU firewalls must be located in locked rooms accessible only to those individuals who are provided access based on tasks assigned. In addition, the room lock must maintain logs of access which can be audited when necessary.
The placement of firewalls in the open area within a general purpose data processing center is prohibited, although placement within separately locked rooms or areas which themselves are within a general data processing center is acceptable.

**Exceptions:**

Administrators seeking exceptions to the Perimeter Firewall Standard will be evaluated on a case-by-case basis by University Information Technology Services.

**Review Schedule:**

The Perimeter Firewall Standard will be reviewed annually by the Office of the CIO or their designee.