Perimeter Firewall Standard

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

**Effective Date:** February 1, 2018

**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 are provided in a secure manner, align with University standards, and removal of legacy exceptions 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 exceptions requests must be sent to the KSU Service Desk at service@kennesaw.edu.

*Default to Deny All*

Every Internet connectivity path and service not specifically permitted by this policy, or documented via a service ticket, will be blocked by the Kennesaw State University Firewall. The current firewall rule base is documented by Office of the CIO Networking and available to all KSU systems administrators.
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 Management
New firewall rule requests will be reviewed by Office of the CIO Networking and Office of Cybersecurity staff and evaluated on 2 factors:

- The request supports the mission of the University
- Applicable security controls have been implemented

Requests which fail to meet these 2 requirements will be reviewed by the Executive Director of Infrastructure Engineering and the Executive Director of Office of Cybersecurity. Requests for new rules will be processed within 24 hours of 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 will be performed by the Office of the CIO’s Office of Cybersecurity.

Logs
All changes to firewall configuration parameters, enabled services, and permitted connectivity must be logged. These logs must be stored on the enterprise log intelligence system and retained in alignment with University standards.

Physical Security
All KSU firewalls must be located in locked rooms accessible only to those individuals who are provided access based on roles. In addition, the room lock must maintain logs of access which can be audited. 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 the Office of the CIO.
Review Schedule:

The Perimeter Firewall Standard will be reviewed annually by the Office of the Chief Information Officer and Vice President for Information Technology or his/her designee.