



Kansas Health Policy Authority Operational Policy

Title: Security Firewall Policy

Number: POL-IT:2008-14

Effective date: 03-17-08

Date Revised: None

Date Modified: None

Date of Annual Review: None

Authority: POL-IT:2007-01

CATEGORY

Information Technology

SUBJECT

Principles of information technology

BACKGROUND

A firewall policy describes how the information security policy will be implemented by the firewall and associated security mechanisms. The firewall policy dictates how the firewall should handle applications traffic such as web, e-mail, or other network traffic. The policy describes how the firewall is to be managed and updated.

All firewall platforms must utilize rulesets as their mechanism for implementing security controls.

Generally speaking, the KHPA network consists of four network segments in addition to an isolated test environment network: the public network, the internal (trusted) network, the DMZ/e-mail network and a secured secondary network segment for housing protected information.

The internal network is considered a trusted network. All devices on it must be KHPA-managed nodes. KHPA workstations and internal-only servers will be on this network. Traffic outbound to the public network must be restricted to allow only traffic needed to support business processes.

The DMZ is only a "semi-trusted" network, and all public traffic entering KHPA's network must be directed to the DMZ unless the connections come from a trusted business partner, secured by Virtual Private Network (VPN). Any public-facing servers must be on the DMZ. The only traffic allowed in to and out of the DMZ is what is required for hosted services, such as e-mail, ftp, and mobile services.

VPNs will be set up to allow only that inbound traffic which is required to support the shared services.

The secondary network is an extension of the internal network but segmented from it to control access to protected information that the KHPA information database administrators/developers control. Administrators, developers and services (applications) that require access to this data are the only hosts that will be allowed connections to this network. Connections into this network will only be allowed from the internal and DMZ network as required. External connections from outside the internal or DMZ are prohibited to the secondary network.

POLICY STATEMENT

The firewall policy must remain consistent with the guiding principles used in the design of the KHPA IT architecture.

Firewall rulesets must be audited and verified by the KHPA Information Technology Director when significant changes occur and no less than annually.

All KHPA vendors that require Virtual Private Network (VPN) access to KHPA network resources must be protected by an encryption level that meets or exceeds Triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES).

The KHPA Information Technology Director evaluates traffic allowed into and out of the network as required for conducting KHPA business. Only the essential traffic to support KHPA business is allowed into the network. Only traffic identified and approved by the KHPA IT Director will be allowed out of the network.

All externally connected firewalls must be implemented on a stateful appliance-based firewall.

Modifications to the firewall rulesets, and the approvals thereof, are tracked using control management and/or workflow management software and are implemented during an acceptable maintenance window as determined by the Information Technology Director.

The Information Technology Director evaluates current firewall upgrades to ensure the modification is stable and reliable before implementing. Updates and upgrades for firewalls must be implemented ensuring compatibility and software integration factors are considered.

All firewall management functions must take place over secured links using strong authentication and encryption.

All KHPA firewalls necessary to regulate the security of the KHPA network must be located in a physically secured area.

Firewall logging must be enabled for all accepted and denied traffic. Logs must be kept for a minimum of six months. All firewalls must be backed up immediately preceding any modification.

Users must not circumvent the firewall by using dial-out modems or network tunneling software to connect to the Internet.

The firewall will protect against address spoofing. The firewall shall not accept traffic on its external interfaces that appear to be coming from internal network addresses.

Anonymous FTP into the Agency's Network will not be allowed.

SPONSOR/CONTACT

Chief Operations Officer