

**Office of the Chief Information Officer
Enterprise Policy**

Policy Number: CIO-076

Effective Date: 01/01/2003

Revision Date: 11/01/2005

Subject: Firewall and Virtual Private Network Administration Policy

Policy Statement: The integrity of the Kentucky Information Highway (KIH) must be protected to ensure uncompromised network services for all connected agencies. The administration of firewalls and virtual private networks (VPN) is a primary component in securing the infrastructure and must conform to the specifications below. Agencies not complying with this policy will lose KIH network services.

Policy Maintenance: The Commonwealth Office of Technology (COT), Office of Infrastructure Services, Division of Communication Services, and Security Administration Branch share the responsibility for maintaining and updating this policy. The revision review cycle for this policy will be annual.

Authority: In accord with KRS 11.507 the Commonwealth Office of Technology (COT) is charged with "Assuring compatibility and connectivity of Kentucky's information systems; developing, implementing, and managing strategic information technology direction, standards, and enterprise architecture, including implementing necessary management processes to assure full compliance....[and] maintaining the technology infrastructure of the Commonwealth.

Responsibility for Compliance: Agencies have an obligation to regularly assess network and computing resources to confirm that they are at an acceptable level of risk from intrusions from the Internet and Intranet. Agencies are responsible for securing sensitive and confidential systems from unauthorized access by Internet and/or Intranet users. All agencies planning to install firewall and/or VPN services must contact COT. Agencies not complying with this firewall and VPN policy will lose KIH network services.

Enterprise Architecture: This Enterprise policy has been approved by the Enterprise Architecture and Standards Committee and constitutes an element of the Security Domain in the Enterprise Architecture.

Policy Detail: COT shall manage all enterprise and intranet firewall and VPN services that utilize the KIH infrastructure. Agencies may manage agency-level Tier II firewall services under certain stipulations and with COT network visibility to the firewall. It is imperative that network services for all agencies within the KIH are protected and that the integrity of the KIH is protected to insure that enterprise services are not compromised. The administration of firewalls and virtual private networks (VPN) is a critical component in securing the KIH infrastructure and computing systems.

In accordance with Enterprise Standards as defined in section 3000 Technology – Network, category 3700, titled Security – Firewall, the approved enterprise products are Checkpoint Firewall-1 and Nortel Contivity appliances for firewall services.

Procedure:

- CheckPoint Firewall-1 product is the approved product for Tier I firewall services. Tier I classification includes all services and/or systems that are considered an enterprise resource. Enterprise resources should be located at the Commonwealth's Data Center (CDC) in order to maximize security benefits and network efficiency. Enterprise resources located at CDC benefit from additional security technologies in place at the CDC.
- Nortel's Contivity firewall product is the enterprise standard for Tier II firewall services. Tier II classification includes all services and/or systems that are agency specific but available for the enterprise. Agency specific applications and services would be suitable for Tier II firewall services. Tier II firewall services may not be interoperable with other enterprise security platforms.

- Internet and Extranet (business relationships) VPN connections must be managed to maintain enterprise security and reduce the security risks. For this reason, COT shall be the approving authority for access to KIH computing resources. Agencies using the Internet to communicate and share data must use the COT-managed VPN service.
- Intranet VPN connections shall be managed by COT to maintain enterprise security and network routing efficiencies. Agencies wanting to create Intranet VPN's must use COT VPN approved services. Nortel's Contivity VPN solution is the approved product for Intranet VPN services.

Exception Process: Because of security risks to the entire KIH, firewalls shall not be implemented without COT approval. A business case exception request must be submitted for consideration before agency deployment. Agencies implementing any firewall(s) without approval shall be disconnected from the KIH.

VPN connections shall be not allowed outside the enterprise firewall unless administered by COT. All non-COT VPN services shall be blocked at the enterprise firewall. Intranet VPNs shall not be constructed without COT approval. Agencies implementing VPNs without COT consent shall be disconnected from the KIH.

Unacceptable Uses: Other activities related to firewall and VPN technologies that could cause congestion and disruption of networks and application services that may cause loss of network connectivity.

END