Policy Title and #	CIO-076: Firewall and Virtual Private Network Administration				
Effective Date:	01/01/2003	Revision Date:	02/04/2021	Review Date:	02/02/2021

POLICY STATEMENT:
The integrity of the Commonwealth of Kentucky's network must be protected to ensure uncompromised IT services for all connected agencies. The administration of firewalls and virtual private networks (VPN) are a primary component in securing the infrastructure and must conform to the specifications below. Agencies not complying with this policy may lose access to the Commonwealth of Kentucky's infrastructure network services.

POLICY MAINTENANCE:
The Commonwealth Office of Technology (COT), Office of Infrastructure Services, Division of Network Services, OCISO, and the Risk & Compliance Branch share the responsibility for maintaining and updating this policy.

REVIEW CYCLE:
This policy will be reviewed at least every two years.

AUTHORITY:
In accord with KRS 42.726 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.

RESPONSIBILITY FOR COMPLIANCE:
COT has an obligation to regularly assess network computing resources to confirm that they are at an acceptable level of risk from intrusions from both internal and external sources. Agencies are responsible for securing sensitive and confidential systems from unauthorized access by internal and external users. Agencies requesting firewall and/or VPN services must use COT as a provider of those services. Agencies not complying with this firewall and VPN policy may lose access to the Commonwealth of Kentucky's infrastructure network services.

POLICY DETAIL:
COT shall manage all Firewall and VPN, services that utilize the Commonwealth of Kentucky's infrastructure. It is imperative that network services for all agencies are protected and that the integrity of the infrastructure network is protected to ensure that enterprise services are not compromised. The administration of firewalls, and virtual private networks is a critical component in securing the infrastructure and computing systems.

- Firewall services are part of a computer system or network that is designed to block unauthorized access while permitting outward communication. Firewall services may not be interoperable with other enterprise security platforms.

- 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 the Commonwealth's computing resources. Agencies using the Internet to communicate and share data must use the COT-managed VPN service.

- 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.

- 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 Commonwealth network.

UNACCEPTABLE USES:
Other activities related to firewall and VPN technologies that could cause congestion and disruption of networks and application services that result loss of network connectivity (reference CIO-090 Information Security Incident Response Policy).

REFERENCES:
Helpful references can be found on the Enterprise IT Policies webpage.