## I. PURPOSE

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.

## II. DEFINITION

1. "Agency" – means any department, program cabinet, institution, board, commission, office, or agency of the state as defined in KRS 11.080 and as the term agency is used in KRS 11.090 to 11.110.

2. "Firewall" – means services that are part of a computer system or network that is designed to block unauthorized access while permitting outward communication.

3. "F5 load balancing services" – means technology that allows monitoring of applications for response time network condition and user content.

## III. POLICY

COT shall manage all Firewall, VPN, F5 load balancing 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 may not be interoperable with other enterprise security platforms.

VPN connections must be managed to maintain enterprise security and reduce 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 not be 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.

1. **Unacceptable Uses**

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

**2. Exemption Requests**

Agencies may request exceptions to this policy by submitting a security exemption request through ServiceNow.

## IV. COMPLIANCE AND DISCIPLINARY ACTION

Each agency must ensure that staff within their organizational authority are made aware of and comply with this policy. The agency is responsible for enforcing it. Failure to comply with this policy may result in disciplinary action up to and including dismissal. COT may require additional service charges for remediation efforts due to non-compliance with this policy.

Agencies that do not comply with this policy may lose access to the Commonwealth of Kentucky's infrastructure network services.

## V. APPLICABILITY

All executive branch agencies and non-executive branch agencies using COT-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government. Organizations may modify this policy to fulfill their responsibilities but must obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification.

## VI. REFERENCES

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

CIO-090 Information Security Incident Response Policy