I. PURPOSE

This policy establishes controls related to Network Security Architecture.

II. POLICY

The Commonwealth Office of Technology (COT) provides and manages the communications network as a shared resource for the Commonwealth of Kentucky. COT shall manage the network and establish zones for appropriate access and security of Commonwealth systems and data. COT also regulates communication methods and protocols over the Commonwealth's network to maximize security and minimize risk.

COT and agencies shall align their resources and access by hosting their systems in the appropriate, COT designated zones. COT segregates the network and resources into these main zones: Intranet, Agency, Server, E-Government (E-GOV), and Extranet.

1. Zones:

a. Intranet: This zone exists behind the Internet firewall and hosts the core shared services container for all consolidated agencies. COT controls all policies and access within this zone.

b. Agency: This zone exists behind the Intranet, hosts various consolidated agencies with their own security zones, and allows the agencies to house their specific services and users. These zones have their own firewalls and related security services separating them from the Intranet zone.

c. Server: This zone is like the Agency zone in that it exists behind the Intranet and separates services from the Intranet zone. This zone houses project-specific firewalls.

d. E-Government (E-GOV): COT uses this zone to provide limited access and services to non-Executive Branch government agencies and their users, such as the Legislative Research Commission, Administrative Office of the Courts, and Secretary of State's Office. Entities in this zone shall provide firewall services for their zone or request firewall services from COT.

e. Extranet: COT uses this zone to provide network access for quasi-state agencies that are not part of the state consolidated infrastructure. COT also provides this zone for external business partners to have limited connectivity into the state network infrastructure.

COT will adhere to best practices by assigning network resources into the appropriate zones whenever possible. COT may modify the use of these zones to tailor security, accessibility, and performance for the services within the zones. Agencies and non-state entities accessing the Commonwealth's network may request exceptions to the placement of resources within the zones; however, COT retains final authority and responsibility for the placement of resources into these zones.

2. Other Restrictions:

COT restricts the use of unencrypted protocols for the means of file transfer. Agencies and users shall encrypt confidential data traversing the Commonwealth's network through approved secure protocols as outlined in the Enterprise Architecture Kentucky Information Technology Standards (KITS).

3. Unacceptable Uses:

Network activities related to technologies such as firewall, load-balancing, high-availability, VPN, etc., that could cause disruption of networks and application services that result in loss of network connectivity (reference CIO-090 Information Security Incident Response Policy) are unacceptable uses. Agencies and staff shall not use unapproved file transfer or storage products. COT prohibits split tunneling, a method that allows access to different security domains—such as a local LAN and a public network—at the same time, using the same or different network connections, for VPN connections.

4. **Exemption Requests:**

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

III. CORRECTIVE OR DISCIPLINARY ACTION

Each agency shall ensure that all relevant staff within their organizational authority are aware of and comply with this policy. The agency is responsible for enforcing it. Unauthorized and/or neglectful actions regarding 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.

IV. 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.

V. REFERENCES

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