COMMONWEALTH OFFICE OF TECHNOLOGY

OFFICE OF THE CHIEF INFORMATION OFFICER ENTERPRISE POLICY

Policy Title and #	**CIO-074: Enterprise Network Security Architecture**				
Effective Date:	**12/01/2002**	Revision Date:	**09/01/2021**	Review Date:	**09/01/2021**

POLICY STATEMENT:

This policy establishes controls related to Network Security Architecture. It provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

DEFINITIONS:

DMZ: An intermediate zone between the Commonwealth's network and the internet used to isolate and protect Commonwealth resources by logically separating the Commonwealth's proprietary network from untrusted networks. This also applies to internal zones that separate an agency's user's LAN from an internal server network.

KITS: Kentucky Information Technology Standards

Split Tunneling: Split tunneling is 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.

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. COT should assign 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.

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.

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.

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

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 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.

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.

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).

Agencies and staff shall not use unapproved file transfer or storage products (e.g., DropBox or SkyDrive).

COT prohibits the use of split tunneling for VPN connections.

AUTHORITY:

KRS 42.726 authorizes COT to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

APPLICABILITY:

All executive branch agencies and non-executive branch agencies using COT-managed infrastructure or services must adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

RESPONSIBILITY FOR COMPLIANCE:

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. 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.

MAINTENANCE:

COT's Office of Infrastructure Services (OIS) and Office of the Chief Information Security Officer (CISO) share responsibility for maintaining this policy. 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.

REVIEW CYCLE:

OIS and CISO will review this policy at least every two years.

REFERENCES:

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