

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

Policy Number: CIO-074

Effective Date: 12/01/2002

Revision Date: 03/17/2015

Reviewed Date: 03/17/2015

Subject: Enterprise Network Security Architecture

Policy Statement: The Commonwealth Office of Technology (COT) is responsible for providing a Commonwealth network architecture and computing environment that enables its customers to protect resources. In order to better protect and secure the resources of the state computing environment, it is necessary to enhance the Enterprise Network Security Architecture and segregate resources and types of activities.

Policy Maintenance: The Commonwealth Office of Technology, Office of Infrastructure Services, Division of Communications, has the responsibility for the maintenance of this policy.

Authority: KRS 42.726 authorizes the Commonwealth Office of Technology (COT) to develop policies that support and promote the effective application of information technology within the executive branch of state government, as well information technology directions, standards, and necessary management processes to assure full compliance with those policies.

Applicability: This policy is to be adhered to by all Executive Branch agencies and staff, including employees, contractors, consultants, temporaries, volunteers and other workers within state government.

Responsibility for Compliance: Each agency is responsible for assuring that staff members under its authority have been made aware of the provisions of this policy, that compliance is expected, and that intentional, inappropriate use of resources may result in disciplinary action up to and including dismissal. It is also each Agency's responsibility to enforce and manage this policy. Failure to comply may result in additional shared service charges to the agency for COT's efforts to remediate issues relating to the lack of adherence to this policy.

Review Cycle: This policy will be reviewed at least every two years.

Policy: COT furnishes the communications backbone for users of the Commonwealth of Kentucky network, an enterprise shared resource. COT and its customers are required to align access and resources in the most appropriate secure zone. In order to better protect and secure the resources of the state's computing environment, it is necessary to enhance the Enterprise Network Security Architecture and segregate resources and types of activities. This architectural change creates six secure domains in the Commonwealth of Kentucky network (listed below).

Secure Zones:

1. **Direct Internet Access Zone:** The Direct Internet Access zone houses the internet access for all other zones. This zone hosts no internal resources, exists outside of the internet firewall, and has limited security.
2. **Extranet Zone:** The Extranet zone supports network connections for agencies that are not part of the state Intranet (consolidated) infrastructure. This zone is mainly used by non-traditional state government agency/users and external business partners. Limited connectivity is offered from this zone into the state network infrastructure for resource access. This zone has limited security and exists outside of the Internet firewall.

3. **E-Government (E-Gov) Zone:** The E-Government (E-Gov) zone is the portion of the state network infrastructure that provides access and services to quasi government agency/users. This zone exists behind the Internet firewall and has limited firewall and security services.
4. **Enterprise DMZ Zone:** The Enterprise DMZ zone provides access to all consolidated public facing servers. This is the only acceptable zone within the state network infrastructure to house servers that can be reached from the Internet. The DMZ resides behind the Internet firewall and has the most restrictive port access of any other zone.
5. **Intranet Zone:** The Intranet zone is the core shared services container for all consolidated agencies, which exists behind the Internet Firewall. COT controls all policies and access within this zone.
6. **Agency Zone:** The Agency zone is used by various consolidated agencies that have their own security zones, housing their specific services and users. These zones have their own firewalls and related security services separating them from the Intranet zone.

Split Tunneling:

The Commonwealth does not allow the use of split tunneling for VPN connections. Split tunneling opens up additional risk by allowing pathways for data that bypass the secure boundaries established to protect the network.

For customers needing assistance on how best to align access and resources, they should contact the Commonwealth Service Desk (CommonwealthServiceDesk@ky.gov or (502) 564-7576).

References:

- CIO-085 – Authorized Agency Contact Enterprise Policy:
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-67586/>

END