

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

Policy Number: CIO-074

Effective Date: 12/01/2002

Revision Date: 11/01/2005

Subject: Enterprise Network Security Architecture

Policy Statement: The Commonwealth Office of Technology (COT) is responsible for providing the Commonwealth network architecture and computing environment that enables our customers to protect their 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.

Responsibility for Compliance: Each agency is responsible for assuring that employees within its organizational authority have been made aware of the provisions of this policy, that compliance by the agency and organization is expected, and that intentional non-compliance may result in a network site being disconnected from the KIH until conformance with this policy.

It is also each Cabinet'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 security and support issues.

Policy Maintenance: This Enterprise Policy has been approved by the Enterprise Architecture and Standards Committee and constitutes an element of the Security Domain in the Enterprise Architecture. The Commonwealth Office of Technology, Office of Infrastructure Services and Office of Enterprise Policy and Project Management share the responsibility for the maintenance of this policy. This policy is to be adhered to by all organizations, agencies and employees that utilize the state network infrastructure and Kentucky Information Highway (KIH).

Policy:

COT furnishes the communications backbone for users of the Kentucky Information Highway (KIH), an enterprise shared resource. 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 three separate network security domains within the KIH infrastructure is necessary to realign resources in the most appropriate security environment. The domains are:

Intranet: The Intranet zone is the private internal network that contains users, internal business systems and most of the remote locations on the state network. The Intranet is protected by a firewall and related security services that provide limited access from outside the internal network. The security systems will utilize a "block all, allow few" approach to each rulebase. Access to the Intranet from external locations will require use of the COT-provided VPN service. This service will also require the use of token-based authentication to ensure high levels of security.

e-Government DMZ: The DMZ is the portion of the state network infrastructure that provides limited firewall services and is designed to support services and/or systems that need access by external users. The DMZ consists of multiple network connections that will allow some diversity in security protection. Additional security protection can be provided in the DMZ zone with dedicated firewall services for servers and server farms. All services and/or systems that need to be publicly accessible must be placed within the DMZ zone.

Extranet: The Extranet zone is outside the Intranet and DMZ zones and supports network connections for agencies that are not part of the state Intranet infrastructure due to their business situation. The Extranet zone

is the connection point to k-12 schools, Post Secondary Education entities, non-traditional state government users and external business partners. This zone also supports the network connection to the Internet.

Procedure:

All customers that utilize the KIH must review their business practices to realign their resources into one of the three security domain zones. All services and systems that need access by users outside the state Intranet must be identified and a list provided, via encrypted email, to COT, OIS, Division of Communications by September 1, 2002. The following information should be included:

- Device/Machine name
- TCP/IP address
- Operating System, including version
- Primary function
- Brief description of the services on the server

Services and systems that need access by users outside the state Intranet must choose and implement one of the following options by December 31, 2002:

Option 1: Move the services and/or systems to the E- Government DMZ zone. The DMZ zone is located at the COT Cold Harbor facility. Servers may be operated by agency staff and incur only the *Server Support: Space Only* charge listed on the COT services list. Agencies may also choose additional server support service levels if needed.

Option 2: Add an additional KIH connection to the site housing to support the services and/or systems. This KIH connection would be separate from the agency's Intranet connection and could not be attached to that connection in any manner. Agencies must manage the services and/or systems new KIH connection in a manner that does not circumvent the security of the Intranet. The KIH connection would be provided at the normal costs associated with a new network location. The KIH connection would be located on the Extranet and have minimal protection via a COT provided multi-agency firewall.

Option 3: Move the services and/or systems to a 3rd party hosting site. This provides connectivity via a remote, non-KIH solution.

Option 4: Move the agency's existing KIH connection outside the Intranet. The KIH connection would be located on the Extranet and have minimal protection via a COT provided multi-agency firewall. Agencies that want to pursue Option 4 must submit a Business Case Exception Request.

On January 1, 2003, COT will implement a "block all, allow few" rulebase on the newly installed Intranet firewall systems. This will limit most traffic to Intranet and require a VPN account and token-based authentication to access internal sites and systems.

**Enterprise Network Security Architecture
Frequently Asked Questions (FAQ's)
June 16, 2002**

Q. This is a big change to the way I deploy and manage systems. Why is it necessary?

A. Various federal requirements for some agencies, as well as oversight authorities such as the Auditor of Public Accounts, require enhanced focus on the protection of valuable resources. Today the network is not segmented into security domains. The current structure is difficult to protect and increases the vulnerability of agency resources. The new design allows more appropriate levels of protection to be employed and reduces the overall risk to internal users and systems.

Q. How does this enhance security for internal users and systems?

A. The Intranet will be protected by firewalls that use a "block all, allow few" approach to the rulebase. This will block most access to everyone except VPN users. This will significantly reduce the risk of virus attacks, hacking attempts and exploitation of system vulnerabilities by external users.

Q. What do I do if have servers that host applications for both internal and external users?

A. You must choose one of the four options or separate the applications onto different servers so you can keep the internal applications at their existing site.

Q. If I move my servers to the DMZ, are they secure?

A. Servers on the DMZ will have the same level of risk and at least the same level of security that is in place today on the enterprise firewall system. COT can work with each agency to assess extra security options on the DMZ. Some can be provided at no cost, but others may require additional security solutions that also have a cost.

Q. Once the secure Intranet is operational; will my internal users and systems be completely safe from vulnerabilities and potential risk?

A. No. You will be better protected from external attacks and exploits; however you may still need additional firewall and security protection to ensure a safe computing environment. Internal Intranet users may still pose some level of risk.

Q. How do I remotely administer my servers from external locations or home when they require after-hours support?

A. A VPN account will be required to access the Intranet in most cases. COT will also provide Intranet dial-up services using token authentication that will allow access to internal resources.

Q. How do I get physical access to my servers if I choose Option 1?

A. COT has 24 hour staffing at the Cold Harbor facility. Agencies can make arrangements for scheduled maintenance access to the building. COT staff can also provide access to authorized customer staff into the building during an emergency situation.

Q. Once the "block all, allow few" firewall policy is implemented, what are the likely services that will be unavailable?

A. It is likely that most services will be unavailable. Enterprise VPN services will be allowed through the firewall. Other services will be reviewed on a case-by-case basis and possibly allowed in a very limited manner.

Q. What is VPN and what does it require?

A. VPN stands for Virtual Private Networking. VPN is a method for giving users a secure way to access KIH resources over the Internet or other public or private networks. For additional information see http://www.state.ky.us/got/ois/security/faq_vpn.htm

Q. What is token-based authentication?

A. Token-based authentication requires a hardware device that provides extra security controls for critical resources. It is designed to make access less vulnerable to unapproved access.

Q. What 3rd party hosting solutions are available?

A. There is currently one contract in place that provides hosting services. It can be found at:
<http://www.state.ky.us/got/contract/commerce.htm>. An RFP has been released for additional hosting services.