Cyber Tree Systems
A Business IT Solution Company

POLICY NAME	**Firewall Internal Security**		
DATE OF LAST REVISION:	9/4/2003	**VERSION NO.**	1.43
ADMINISTRATOR RESPONSIBLE	Kevin McKnight		

Purpose

This policy establishes information security requirements for all networks and equipment deployed in CTS located on the internal network. Adherence to these requirements will minimize the potential risk to CTS from the damage to its public image caused by unauthorized use of CTS resources, and the loss of sensitive/company confidential data and intellectual property.

Scope

CTS networks and devices (including but not limited to routers, switches, hosts, etc.) that are Intra-network facing and located inside CTS corporate Internet firewalls are considered part of the internal network and are subject to this policy. All existing and future equipment, which falls under the scope of this policy, must be configured according to the referenced documents.

Policy Statement

- Ownership and Responsibilities
  - All new equipment must accompany a business justification with sign-off at the business unit Vice President level. InfoSec must keep the business justifications on file.
  - Departments are responsible for assigning managers, point of contact (POC), and back up POC for each department and must maintain up to date POC information with InfoSec [and the corporate enterprise management system, if one exists]. Managers or their backup must be available around-the-clock for emergencies.
  - Changes to the connectivity and/or purpose of existing network equipment and establishment of new equipment connectivity must be requested through a CTS Network Support Organization and approved by InfoSec.
  - A Network Support Organization must maintain a firewall device between the production environment and the DMZ.
  - The Network Support Organization and InfoSec reserve the right to interrupt device connections if a security concern exists.
  - The IS/IT/InfoSec staff will provide and maintain network devices deployed in the network up to the Network Support Organization point of demarcation.

  - The IS/IT/InfoSec staff must record all equipment address spaces and current contact information [in the corporate enterprise management system, if one exists].

  - The Department Managers are ultimately responsible for their organizations complying with this policy.

  - Immediate access to equipment and system logs must be granted to members of InfoSec and the Network Support Organization upon request, in accordance with the Audit Policy.

  - Individual accounts must be disabled within three (3) days when access is no longer authorized. Group account passwords must comply with the Password Policy and must be changed within three (3) days from a change in the group membership.

  - InfoSec will address non-compliance waiver requests on a case-by-case basis.

- General Configuration Requirements
  - Production resources must not depend upon resources outside of the corporate network.

  - CTS's corporate internal networks may not be accessed, either directly or via a wireless connection, by resources or devices outside of the production environment.

  - Network equipment should be in a physically separate room from any DMZ-connected devices. If this is not possible, the equipment must be in a locked rack with limited access. In addition, the Department Manager must maintain a list of who has access to the equipment.

  - Department Managers are responsible for complying with the following related policies:
    - Password Policy
    - Wireless Communications Policy
    - Anti-Virus Policy
    - Cloud Services Policy

  - The Network Support Organization maintained firewall devices must be configured in accordance with least-access principles and the department business needs. All firewall filters will be maintained by InfoSec.

  - The firewall device must be the only access point between the DMZ and the rest of CTS's networks and/or the Internet. Any form of cross-connection which bypasses the firewall device is strictly prohibited.

  - Original firewall configurations and any changes there to must be reviewed and approved by InfoSec (including both general configurations and rule sets). InfoSec may require additional security measures as needed.

  - Access to resources on CTS’s network will be granted based on Extended Access Control Lists (Extended ACLs), which will utilize a most restrictive logic combining source & destination IP addressing and protocol level filtering.

- InfoSec staff will be responsible for configuring and updating Extended ACLs on CTS's internal firewall equipment connected to production level resources.
- All routers and switches not used for testing and/or training must conform to the Network Router and Switch standardization documents.
- Current applicable security patches/hot fixes for any applications must be applied. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
- All applicable security patches/hot fixes recommended by the vendor must be installed. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
- Services and applications not serving business requirements must be disabled.
- CTS Confidential information is prohibited on equipment where non-CTS personnel have physical access (e.g., training labs), in accordance with the Information Sensitivity Classification Policy.
- Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.

Enforcement

Any employee found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

Terms and Definitions

Define any acronyms, jargon, or terms that might have multiple meanings.

TERM	DEFINITION
Access Control List (ACL)	Lists kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).
Extended ACL	Lists kept by routers to control access to or from the router for several services. These access lists specifically filter packets based on source & destination IP address as well as applicable protocol and are usually applied closest to the source of the packet, for most effective filtering (for example, to prevent packets with a certain IP address from leaving a particular interface on the router destined for a specific address using a specific protocol like telnet; port 23).
DMZ (de-militarized zone)	Networking that exists outside of CTS primary corporate firewalls, but is still under CTS administrative control.
Network Support Organization	Any InfoSec-approved support organization that manages the networking of non-lab networks.
Least Access Principle	Access to services, hosts, and networks is restricted unless otherwise permitted.
Internet Services	Services running on devices that are reachable from other devices across a network. Major Internet services include DNS, FTP, HTTP, etc.

Network Support Organization Point of Demarcation	The point at which the networking responsibility transfers from a Network Support Organization to the DMZ Lab. Usually a router or firewall.
Firewall	A device that controls access between networks, such as a PIX, a router with access control lists, or a similar security device approved by InfoSec.
Internally Connected Lab	A lab within CTS's corporate firewall and connected to the corporate production network.

Revision History

Revisions made 9/4/2023