Definitions

File Transfer Protocol (FTP): Is a standard Internet protocol for transmitting files between computers on the Internet.

Overview

The servers at {COMPANY-NAME} provide a wide variety of services to internal and external users, and many servers also store or process sensitive information for {COMPANY-NAME}. These hardware devices are vulnerable to attacks from outside sources which require due diligence by the IT Department to secure the hardware against such attacks.

Purpose

The purpose of this policy is to define standards and restrictions for the base configuration of internal server equipment owned and/or operated by or on {COMPANY-NAME}'s internal network(s) or related technology resources via any means. This can include, but is not limited to, the following:

- Internet servers (FTP servers, Web servers, Mail servers, Proxy servers, etc.)
- Application servers
- Database servers
- File servers
- Print servers
- Third-party appliances that manage network resources

This policy also covers any server device outsourced, co-located, or hosted at external/third-party service providers, if that equipment resides in the {COMPANY-NAME}.org domain or appears to be owned by {COMPANY-NAME}.

The overriding goal of this policy is to reduce operating risk. Adherence to the {COMPANY-NAME} Server Security Policy will:

- Eliminate configuration errors and reduce server outages
- Reduce undocumented server configuration changes that tend to open up security vulnerabilities
- Facilitate compliance and demonstrate that the controls are working
- Protect {COMPANY-NAME} data, networks, and databases from unauthorized use and/or malicious attack

Therefore, all server equipment that is owned and/or operated by {COMPANY-NAME} must be provisioned and operated in a manner that adheres to company defined processes for doing so.

This policy applies to all {COMPANY-NAME} company-owned, company operated, or company controlled server equipment. Addition of new servers, within {COMPANY-NAME} facilities, will be managed at the sole discretion of IT. Non-sanctioned server installations, or use of unauthorized equipment that manage networked resources on {COMPANY-NAME} property, is strictly forbidden.

Policy Detail

Responsibilities

{COMPANY-NAME}'s VP of IT has the overall responsibility for the confidentiality, integrity, and availability of {COMPANY-NAME} data.

Other IT staff members, under the direction of the Director of IT, are responsible for following the procedures and policies within IT.

Supported Technology

All servers will be centrally managed by {COMPANY-NAME}'s IT Department and will utilize approved server configuration standards. Approved server configuration standards will be established and maintained by {COMPANY-NAME}'s IT Department.

All established standards and guidelines for the {COMPANY-NAME} IT environment are documented in an IT storage location.

- The following outlines {COMPANY-NAME}'s minimum system requirements for server equipment supporting {COMPANY-NAME}'s systems.
- Operating System (OS) configuration must be in accordance with approved procedures.
- Unused services and applications must be disabled, except where approved by the Director of IT or the VP of IT.
- Access to services must be logged or protected though appropriate access control methods.
- Security patches must be installed on the system as soon as possible through
- {COMPANY-NAME}'s configuration management processes.

- Trust relationships allow users and computers to be authenticated (to have their identity verified) by an authentication authority. Trust relationships should be evaluated for their inherent security risk before implementation.
- Authorized users must always use the standard security principle of “Least Required Access” to perform a function.
- System administration and other privileged access must be performed through a secure connection. Root is a user account that has administrative
- privileges which allows access to any file or folder on the system. Do not use the root account when a non-privileged account will do.
- All {COMPANY-NAME} servers are to be in access-controlled environments.
- All employees are specifically prohibited from operating servers in environments with uncontrolled access (i.e. offices).

This policy is complementary to any previously implemented policies dealing specifically with security and network access to {COMPANY-NAME}’s network.

It is the responsibility of any employee of {COMPANY-NAME} who is installing or operating server equipment to protect {COMPANY-NAME}’s technology based resources (such as {COMPANY-NAME} data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in the loss of member information, damage to critical applications, loss of revenue, and damage to {COMPANY-NAME}’s public image. Procedures will be followed to ensure resources are protected.