Approved 12/14/11

Texas Wesleyan Firewall Policy

PURPOSE

Firewalls are an essential component of the Texas Wesleyan information systems security infrastructure. Firewalls are defined as security systems that control and restrict network connectivity and network services. Firewalls establish a control point where access controls may be enforced. Connectivity defines which computer systems are permitted to exchange information. A service is sometimes called an application, and it refers to the way for information to flow through a firewall. Examples of services include file transfer protocol (FTP) and web browsing (HTTP). This policy defines the essential rules regarding the management and maintenance of firewalls at Texas Wesleyan and it applies to all firewalls owned, rented, leased, or otherwise controlled by Texas Wesleyan employees.

SCOPE

This policy applies to all firewalls on Texas Wesleyan networks, whether managed by employees or by third parties. Departures from this policy will be permitted only if approved in advance and in writing by the IT Infrastructure Services Director.

In some instances, systems such as routers, air gaps, telecommunications front ends, or gateways may be functioning as though they are firewalls when they are not formally known as firewalls. All Texas Wesleyan systems playing the role of firewalls, whether they are formally called firewalls, must be managed according to the rules defined in this policy. In some instances this will require that these systems be upgraded so that they support the minimum functionality defined in this policy.

SPECIFIC REQUIREMENTS

Required Documentation - Prior to the deployment of every Texas Wesleyan firewall, a diagram of permissible paths with a justification for each, and a description of permissible services accompanied by a justification for each, must be submitted to the IT Infrastructure Services Director. Permission to enable such paths and services will be granted by the IT Infrastructure Services Director only when these paths or services are necessary for important business reasons, and sufficient security measures will be consistently employed. The conformance of actual firewall deployments to the documentation provided will be periodically checked by the Security Engineer or his/her designee. Any changes to paths or services must go through this same process as described below.

Default To Denial - Every connectivity path and service that is not specifically permitted by this policy and supporting documents issued by the Information Technology department must be blocked by Texas Wesleyan firewalls. The list of currently approved paths and services must be documented and distributed to all system administrators with a need to know by the Information Technology department. An inventory of all access paths into and out of Texas Wesleyan internal networks must be maintained by the Information Technology department.

Connections Between Machines - Real-time connections between two or more Texas Wesleyan computer systems must not be established or enabled unless the Information Technology department has determined that such connections will not unduly jeopardize information security. In many cases, firewalls or similar intermediate systems must be employed. This requirement applies no matter what the technology employed, including wireless connections, microwave links, cable modems, integrated services digital network lines, and digital subscriber line connections. Any connection between an in-house Texas Wesleyan production system and any external computer system, or any external computer network or service provider, must be approved in advance by the Information Technology department.

Regular Testing - Because firewalls provide such an important control measure for Texas Wesleyan networks, their strength and proper configuration must be tested on a regular basis. Where vendor software supports it, this testing must include the use of software agents that automatically check to determine whether firewalls remain configured and running in a manner that is consistent with both Texas Wesleyan security policies and the Texas Wesleyan Information Architectural plan. This testing process must include consideration of defined configuration parameters, enabled services, permitted connectivity paths, current administrative practices, and adequacy of the deployed security measures. These tests must include the regular execution of vulnerability identification software and the regular performance of penetration tests. These tests must be performed by technically proficient persons, either in the Information Technology department or working for a third-party contractor. Those responsible for either the administration or management of the involved firewalls must not perform these tests.

Logs - All changes to firewall configuration parameters, enabled services, and permitted connectivity paths must be logged. All suspicious activity that might be an indication of either unauthorized usage or an attempt to compromise security measures also must be logged. The integrity of these logs must be protected with checksums, digital signatures, encryption, or similar measures. These logs must be promptly removed from the recording systems and stored in a physically protected container for at least six months after the time they were recorded. These logs must be reviewed periodically to ensure that the firewalls are operating in a secure manner.

Intrusion Detection - All Texas Wesleyan firewalls must include intrusion detection systems approved by the Information Technology department. Each of these intrusion detection systems must be configured according to the specifications defined by the Information Technology department. Among other potential problems, these intrusion detection systems must detect unauthorized modifications to firewall system files, and detect denial of service attacks in progress. Such intrusion detection systems must also immediately notify by pager the technical staff that is in a position to take corrective action. All technical staff working on firewalls must be provided with remote access systems and privileges so that they can immediately respond to these incidents even when they are physically removed from the firewall.

Contingency Planning - Technical staff working on firewalls must prepare and obtain Information Technology department approval for contingency plans that address the actions to be taken in the event of various problems including system compromise, system malfunction, system crash, system overload, and Internet service provider unavailability. These contingency plans must be kept current to reflect changes in the Texas Wesleyan information systems environment. These plans must be periodically tested to ensure that they will be effective in restoring a secure and reliable networking environment.

External Connections - All in-bound real-time Internet connections to Texas Wesleyan internal networks or multi-user computer systems must pass through a firewall before users can reach a logon banner. Aside from personal computers that access the Internet on an outbound single-user session-by-session dial-up basis, no Texas Wesleyan computer system may be attached to the Internet unless it is protected by a firewall. The computer systems requiring firewall protection include web servers, electronic commerce servers, and mail servers. All personal computers with digital subscriber line or cable modem connectivity must employ a firewall approved by the Information Technology department. Wherever a firewall supports it, logon screens must have a notice indicating that the system may be accessed only by authorized users, users who log on represent that they are authorized to do so, unauthorized system usage or abuse is subject to disciplinary action including criminal prosecution, and system usage will be monitored and logged.

Extended User Authentication - Inbound traffic, with the exception of Internet electronic mail, regular news distributions, and push broadcasts previously approved by the Information Technology department, that accesses Texas Wesleyan networks through a firewall must in all instances involve extended user authentication measures approved by the Information Technology department.

Virtual Private Networks - To prevent unauthorized disclosure of sensitive and valuable information, all inbound traffic, with the exception of Internet mail, approved news services, and push broadcasts, that accesses Texas Wesleyan networks must be encrypted with the products approved by the Information Technology department. These connections are often called virtual private networks (VPNs). The VPNs permissible on Texas Wesleyan networks combine extended user authentication functionality with communications encryption functionality [https:\\uconnect.txwes.edu].

Firewall Access Mechanisms - All Texas Wesleyan firewalls must have unique passwords or other access control mechanisms. The same password or access control code must not be used on more than one firewall. Whenever supported by the involved firewall vendor, those who administer Texas Wesleyan firewalls must have their identity validated through extended user authentication mechanisms. In certain high security environments designated by the IT Infrastructure Services Director, such as the Texas Wesleyan Internet commerce site, remote access for firewall administrators is prohibited. All firewall administration activities must take place in person and on site.

Firewall Access Privileges - Privileges to modify the functionality, connectivity, and services supported by firewalls must be restricted to a few technically-trained individuals with a business need for these same privileges. Unless permission from the IT Infrastructure Services Director has been obtained, these privileges must be granted only to individuals who are full-time permanent employees of Texas Wesleyan, and not to temporaries, contractors, consultants, or outsourcing personnel. All firewalls must have at least two staff members who are adequately trained to make changes, as circumstances require. Such training includes periodic refresher

training course or conference attendance to permit these staff members to stay current with the latest developments in firewall technology and firewall operations. Care must be taken to schedule out-of-town vacations so that at least one person capable of effectively administering the firewall is readily available at all times.

Secured Subnets - Portions of the Texas Wesleyan internal network that contain sensitive or valuable information, such as the computers used by the Human Resources department, should employ a secured subnet. Access to this and other subnets should be restricted with firewalls and other access control measures. Based on periodic risk assessments, the Information Technology department will define the secured subnets required in the Information Architecture.

Demilitarized Zones - All Internet commerce servers including payment servers, database servers, and web servers must be protected by firewalls, and be located within a demilitarized zone (DMZ), a subnet that is protected from the Internet by one or more firewalls. An internal network, such as an intranet, is also protected from the DMZ subnet by one or more firewalls.

Network Management Systems - Firewalls must be configured so that they are visible to internal network management systems. Firewalls also must be configured so that they permit the use of remote automatic auditing tools to be used by authorized Texas Wesleyan staff members. Unless deliberately intended as a test, such automatic auditing tools must not trigger a response sequence through firewall-connected intrusion detection systems.

Disclosure Of Internal Network Information - The internal system addresses, configurations, products deployed, and related system design information for Texas Wesleyan networked computer systems must be restricted such that both systems and users outside the Texas Wesleyan internal network cannot access this information.

Secure Backup - Current offline back-up copies of firewall configuration files, connectivity permission files, firewall systems administration procedural documentation files, and related files must be kept close to the firewall at all times. A permissible alternative to offline copies involves online encrypted versions of these same files. Where systems software permits it, the automatic reestablishment of approved copies of these systems files must proceed whenever an unauthorized modification to these files has been detected.

Virus Screening and Content Screening - Virus screening software approved by the Information Technology department must be installed and enabled on all Texas Wesleyan firewalls. Because the files passing through a firewall may be encrypted or compressed, firewall-based virus detection systems may not detect all virus-infected files. For this reason, virus-screening software is also required at all Texas Wesleyan mail servers, departmental servers, and desktop personal computers. Both content screening software and software that blocks users from accessing certain non-business web sites must also be enabled on all Texas Wesleyan firewalls.

Firewall Dedicated Functionality - Firewalls must run on dedicated machines that perform no other services, such as acting as a mail server. Sensitive or critical Texas Wesleyan information must never be stored on a firewall. Such information may be held in buffers as it passes through a firewall. Firewalls must have only the bare minimum of operating systems software resident and enabled on them. Where the supporting operating system permits it, all unnecessary and unused systems software must be removed from firewalls. Texas Wesleyan does not permit its internal information to be resident on or processed by any firewall, server, or other computer

that is shared with another organization at an outsourcing facility. Outsourcing organization-provided shared routers, hubs, modems, and other network components are permissible.

Firewall Change Control - Because they support critical Texas Wesleyan information systems activities, firewalls are considered to be production systems. All changes to the firewall software provided by vendors, excluding vendor-provided upgrades and patches and fixes must go through the Change Management Process. A firewall policy, defining permitted and denied services and connections, should be documented and reviewed at least twice a year by the Security Engineer. Major changes to the Texas Wesleyan internal networking environment, any changes to the production business applications supported, and any major information security incident must trigger an additional and immediate review of the firewall policy. The same documentation that is required for changes on production systems must also be prepared for firewall changes.

Posting Updates - Texas Wesleyan firewalls must be running the latest release of software to repel these attacks. Where available from the involved vendor, all Texas Wesleyan firewalls must subscribe to software maintenance and software update services. Unless approved in advance by the IT Infrastructure Services Director, staff members responsible for managing firewalls must install and run these updates within two business days of receipt.

Monitoring Vulnerabilities - Texas Wesleyan staff members responsible for managing firewalls should stay current with information about firewall vulnerabilities. Any vulnerability that appears to affect Texas Wesleyan networks and systems must promptly be brought to the attention of the IT Infrastructure Services Director.

Standard Products - Unless advance written approval is obtained from the IT Infrastructure Services Director, only those firewalls appearing on the list of approved vendors and products may be deployed with Texas Wesleyan networks. All firewall interfaces and features deployed, such as virus screening, must be consistent with the Information Architecture issued by the Information Technology department.

Firewall Physical Security - All Texas Wesleyan firewalls must be located in locked rooms accessible only to those who perform authorized firewall management and maintenance tasks approved by the IT Infrastructure Services Director. The placement of firewalls in an open area within a general purpose data processing center is prohibited, although placement within separately locked rooms or areas, which themselves are within a general data processing center is acceptable. These rooms must be equipped with alarms and an automated log of all persons who gain entry to the room.