


Name of Policy: <u>Boundary security.</u> Policy Number: 3364-65-14 Approving Officer: President Responsible Agent: Vice President of Information Technology Scope: all University campuses		 Original effective date: May 28, 2009	
<input checked="" type="checkbox"/>	New policy proposal	<input type="checkbox"/>	Minor/technical revision of existing policy
<input type="checkbox"/>	Major revision of existing policy	<input type="checkbox"/>	Reaffirmation of existing policy

(A) Policy statement

Information technology will maintain robust network perimeter defense systems to provide effective boundary security intended to protect sensitive information and insure the availability, integrity, and confidentiality of the university's information technology resources.

(B) Purpose

This policy requires information technology to implement and operate robust network perimeter defense systems and prescribes boundary security measures that will assist in the isolation and protection of university-controlled information technology resources.

(C) Scope

The scope of this information technology policy includes university computer and telecommunications systems and the employees, contractors, temporary personnel and other agents of the university who use and administer such systems.

(D) Requirements

The core principle of boundary security is: "Allow authorized traffic and deny everything else." To this end, information technology and university organizations shall:

- (1) Establish and protect the network perimeter(s) and facilitate the protection of internal network zones housing and processing sensitive data in accordance with organizational risk assessments as defined in The University of Toledo "Information Security Framework."
- (2) Provide secure remote access through the perimeter for authorized users. Remote access users must be authenticated against the authorized access list in accordance with the "Remote Access Security" policy.
- (3) Incorporate generally prescribed system hardening techniques. Organizations shall determine which ports and services are required to support their business processes and internal system interconnectivity, limit access to these access

points, and disable all others. Organizations shall coordinate with information technology to identify the types of services and protocols permitted both within the network and that cross network boundaries. Some clear text services that cross the network boundaries, such as file transfer protocol (FTP), provide convenience to the user but carry significant risk to the network. Security measures for services and protocols that cross network boundaries include, but are not limited to:

- (a) Servers or firewalls configured specifically to protect against vulnerabilities
 - (b) Host-to-host management
 - (c) Internet protocol (IP) specification for source and destination
 - (d) Strong authentication
 - (e) Encryption
 - (f) Packet filtering
 - (g) Activity logging
 - (h) Virtual Private Network (VPN)
 - (i) System and application software security fixes and patches
 - (j) Using secured (encrypted) alternatives to clear text services and protocols (example: the use of SSH instead of telnet or the use of SFTP instead of FTP.)
- (4) Authentication measures and procedures. Ensure that appropriate authentication measures and procedures are in place for traffic that crosses university boundaries. Authentication measures shall be consistent with the results of the risk assessment as defined in The University of Toledo “Information Security Framework.”
- (a) Use protocols that do not transmit clear text, re-usable authentication information across organizational boundaries.
 - (b) Two-factor authentication may be implemented to limit access to systems that contain data requiring more secure access or information whose disclosure would cause serious disruption or harm.
- (5) Control network traffic. At a minimum, the following functions shall be provided:
- (a) Isolate and protect public and private World Wide Web (Web) services by installing in a demilitarized zone (DMZ).
 - (b) Use DMZ security control for network traffic entering and leaving the network and crossing security boundaries.
 - (c) Establish and protect internal enclaves as required to protect sensitive data by establishing internal security control points using technologies such as firewalls.

- (d) Per the organization's risk assessment, block unwanted traffic such as:
 - (i) Dynamic content, including unsigned Java applets or ActiveX controls.
 - (ii) Multipurpose Internet Multimedia Extensions (MIME) types.
 - (iii) Application specific commands, such as the HTTP "delete" command.
- (e) Route incoming and outgoing traffic to internal systems that are protected.
- (f) Hide vulnerable systems and information from the Internet, such as:
 - (i) IP addresses and local network traffic.
 - (ii) Network topology.
 - (iii) Internal user IDs and account properties.
 - (iv) Configuration details for firewalls and other network security devices.
 - (v) Physical security information for important network devices such as file servers and routers.
 - (vi) Continuity of operations, security assessment reports and disaster recovery plans.
- (6) Monitor attempted probes, attacks or intrusions. All repeated attempts from non-authorized entities to breach the boundary shall be monitored. Information technology shall activate and review logs pursuant to the security audit logging requirements of university policy for "Security Incident Response" and report any evidence of an attack or intrusion as specified by the organization's incident reporting procedures.
- (7) Provide a common, standardized network time source. If systems do not accommodate accepting external network times, upgrades to these systems shall be able and configured to do so.

In addition to serving as an important element in data accuracy, the time mechanisms of the various system components must be synchronized for security reasons. Accurate, synchronized time logs are crucial for tracking a hacker's movements through a system that the hacker has targeted.

(E) Definitions

- (1) Access point. In this context, any point at which an entity outside the boundary connects to the network that contains secured assets.
- (2) Boundary. The perimeter where security controls are in effect to protect assets.
- (3) Demilitarized Zone (DMZ). A computer host or small network established as a "neutral zone" between two networks or network segments to control direct

access to data and other resources. The DMZ mediates communication between assets and creates a boundary security according to locally established security and access control policies.

- (4) Encryption. The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
- (5) File Transfer Protocol (FTP). An inherently unsecured (non-encrypted) service that allows computer-to-computer communication to exchange files directly, regardless of the platforms used. FTP can be accessed through either dial-up modems or the Internet. Secured file transfer protocols such as SFTP or FTPS should be used instead.
- (6) Firewall. Either software or a combination of hardware and software, that implements security policy by governing traffic between two or more networks or network segments. Firewalls are used to protect internal networks, servers and workstations from unauthorized users or processes. Firewalls have various configurations, from stand-alone servers to software on a notebook computer, and must be configured properly to enable protection.
- (7) Two-factor authentication. Authentication that incorporates two elements. There are three elements of authentication: “what you know” (for example, a password or PIN), “what you have” (for example, a digital certificate or a smart card), and “what you are” (for example, a biometric). Two-factor authentication is commonly used for access to systems that contain data requiring secured access or information of which disclosure would cause serious disruption or harm. It is also known as strong authentication, although strong authentication can have more than two elements.
- (8) Virtual Private Network (VPN). Uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

<p>Approved by:</p> <p><u>/s/ laj</u> Lloyd A. Jacobs, M.D. President</p> <p><u>June 11, 2009</u> Date</p> <p>Review/Revision Completed by: Vice President of Information Technology</p>	<p>Policies Superseded by This Policy:</p> <p>Initial effective date: May 28, 2009 Review/Revision Date: Next review date: May 28, 2012</p>
--	---