West Texas A&M University™

The Division of Information Technology
University Information Security Standards

NIST CONTROL FAMILY
IDENTIFICATION AND AUTHENTICATION CONTROLS

CONTROL NUMBER	CONTROL NAME	PRIORITY	REVIEW DATE
SC-7	**Boundary Protection**	**P1**	**07/23/2017**

I. STATEMENT

The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

II. APPLICABILITY

This Control applies to all West Texas A&M network information resources. The intended audience for this Control includes all information resource owners, custodians, and users of information resources.

III. IMPLEMENTATION

All connectivity between University information resources and the Internet will be provided solely by the Network Services division of the Information Technology Department. Individual divisions, departments, and/or colleges shall not establish independent Internet connectivity without the express prior approval of the Information Resources Manager/Chief Information Officer ("IRM/CIO").

Network Services shall ensure that all connectivity between a University information resource and the Internet passes through one or more firewalls ("University Firewall(s)").

The default ruleset for any new University Firewall will be to deny all inbound

traffic and allow all outbound traffic. Only Network Services shall make changes to the ruleset of a University Firewall. Every change to a University firewall ruleset shall be narrowly tailored, i.e., changes shall apply only to those ports, services, users, hosts, etc., that need the change. Network Services shall make a change to a University Firewall ruleset only pursuant to a written request approved, at a minimum, by the IRM or his/her designee(s). In emergency situations, Network Services may make changes (e.g., blocking of certain types of inbound or outbound traffic) to a University firewall ruleset without a written request or IRM approval. Network Services shall document each and every change made to a University Firewall ruleset. Network Services shall periodically review all University Firewall rulesets to determine whether any changes need to be made or reversed.

Network Services shall enable alarm, alert, and audit logging functions on all University Firewalls and shall be responsible for the monitoring and analysis of log files generated.

Periodic audits of University Firewall rulesets, firewall change documentation, and firewall log files shall be conducted.

All University Firewalls shall be located in a physically secure location, the access to which shall be controlled by the Information Technology Department.