Effective: February 21, 2017

Information Technology Policy
FIREWALL

Approved: February 21, 2017
President's Cabinet

Introduction

Millersville University manages internal and external firewalls to establish a secure environment for the University's network and computer resources. These firewalls filter internet traffic to mitigate the risks and potential losses associated with security threats to the University's network and information systems. Millersville University firewalls establish a control point where access controls may be enforced.

While responsibility for information systems security on a day-to-day basis is the responsibility of the entire University community, specific guidance and direction for information systems security is the responsibility of IT. The Networking and Systems teams within the University's IT department are responsible for implementing, configuring, and maintaining the University's firewalls.

Purpose

The purpose of this policy is to define standards for provisioning security devices owned and/or operated by Millersville University. These standards are designed to minimize the potential exposure of Millersville University to the loss of confidential data, intellectual property, and damage to public image, which may result from unauthorized user of Millersville University resources.

Policy

Where electronic equipment is used to capture, process, or store University data classified as Confidential, and the electronic equipment is accessible via a direct or indirect internet connection, a firewall that is appropriately installed, configured, and maintained is required.

Where electronic equipment is used to capture, process, or store University data classified as University Restricted or Public, and the electronic equipment is accessible via a direct or indirect internet connection, a firewall that is appropriately installed, configured, and maintained is recommended.

Operational Procedures

1. The University's perimeter firewall permits the following outbound and inbound Internet traffic:

   A. Outbound – All internet traffic to hosts and services outside of Millersville University's networks except those specifically identified and blocked as malicious sites.

   B. Inbound – Internet traffic that supports the mission of the University and is in accordance with defined policies.

2. In order to protect Millersville University's networks and users, some ports and applications may be filtered.

3. Where the risk is acceptable, granting of firewall exception requests will be dependent on the network infrastructure limitations and the availability of required resources to implement the request. If the risk associated with a request is not deemed acceptable, an explanation of the associated risks will be provided to the requestor and alternative solutions with be explored.

   A. Appeals may be made to the CIO.

4. A unique identity which can be logged, is required to access, read, or write firewall configurations by Network and Systems team members.

   A. Configuration changes to the firewall must follow the appropriate procedures in accordance with the University's Change Management Policy.

      a. All updates to existing rules can be scheduled outside the change management process.

Review

Firewall installations and rule-sets will be reviewed on a bi-annual basis by the Network and Systems and Information System Services team.