Information Security Standard: Network Security

Revision History:

Date	By	Action	Pages
09/30/10	Madjedi	Release of New Document	All

Review Frequency:

Annually

Responsible Office:

ITS OCIO

Responsible Officer:

Vice-Provost ITS/CIO

Brief Description:

This standard describes the requirements for placement of assets on the campus network, access to the campus network, transport of data across the network and management of the network against security threats.

Related Policy:

CSU Information Security Policy
- 8045.0 – Information Technology Security
- 8060.0 – Access Controls

Cal Poly Information Security Program

Introduction:

Controls are in place through policy, standards, guidelines and practices to support of the purpose of Cal Poly's Information Security Program. Various sets of controls are required to protect information contained on computing devices connected to the university's network. These controls are determined based on the classification of the data, services provided and associated risk to the university if these assets were compromised.

Controls established through policy and standards specific to computing devices on campus protect against vulnerabilities such as:

- Weak physical security
- Vulnerabilities in Software (operating system and/or application)
- Unsecured Configuration / Mis-Configuration
- Inappropriate user access configurations (e.g. access too broad, no longer used, etc.)
- Poor user practices (e.g. easily cracked passwords, saving confidential data on unprotected computers, installing software from a non-trusted source, etc.)

Scope:

The following network security standard identifies requirements that enhance the protection against, and detection of security threats.   CSU ITRP Baseline Network Standard Architecture defines a 'defense in depth' strategy utilizing network zones to organize

- the placement of information and computing resources on the network
- manage appropriate access to those resources and
- enable protection and detection management of threats and attacks on those resources.

This standard follows the same principles.

Standard:

Required:

1) Boundary Protection: The campus network interface to the public network is configured to deny traffic inbound to the campus network by default and allow inbound network traffic by exception following the ITS Firewall Pinhole request process.
2) Asset placement on the network:
    a. High Risk Enterprise Devices must be attached to the network such that the asset resides in a Critical Services Zone identified by ITS Network Administration.
    b. A Critical Services Zone must
        i. ensure that network traffic to and from a device in the zone can be restricted using a CSU ITRP Standard firewall. This includes traffic in and out of the Critical Services Zone and between computing devices within the zone itself.
        ii. deny network traffic by default and allow network traffic by exception.
    c. All university and auxiliary organization owned assets must be registered (IP Address Request) with ITS Network Administration before connecting to the campus network.
    d. University and auxiliary organization owned assets connecting to the Trusted Asset Zone must comply with university configuration and maintenance standards.
    e. Non-Cal Poly or non-auxiliary owned assets connecting to the network must connect using the Public User Access Zone .
3) Access: Access to the Cal Poly network must be authenticated at a user level with a unique identifier.
4) Transport: Level 1 data must be transported across the campus network following Information Security Device Standard for encryption.
5) Management:
    a. Network traffic in support of the management of networking devices must be logically segmented into a Network Management Zone. Access to the Network Management Zone is restricted to authorized devices used for Network Management purposes.
    b. Network traffic is monitored for unusual or unauthorized activities or conditions at interfaces with Critical Network Zones and the campus network border.

Recommended:

1) Asset placement on the network: Enterprise devices should be attached to the network such that the asset resides in a Critical Services Zone identified by ITS Network Administration.

Definitions:

Critical Asset Zone

A collection of High Risk Enterprise devices that are grouped together and segmented from the rest of the campus network via perimeter and access controls.

Trusted Asset Zone

A collection of university or auxiliary owned assets connected to the campus network that

- are included in the scope of campus security device standards and
- do not contain Level 1 data in a persistent manner and
- are connected to network segments designated for trusted assets.

Public User Access Zone

A collection of non-university or non-auxiliary owned assets connected to the campus network on segments designated for assets **not** specifically configured or managed following campus device standards.

Responsibilities:

ITS-Network Administration

- Responsible for implementation and management of network based controls in association with this standard.
- Responsible for communicating to the campus appropriate connection points (zones) based on this standard.

Computing Device Administrators/Application Administrators

- Ensures devices are placed on the network in compliance with this standard.
- Communicates with application users the capability of the application to encrypt appropriate data when transported across the network.
- Responsible for registering devices with Network Administration before placement on the network.
- Responsible for updating device registration information following the university network asset review process.

Computing Device Users

- Responsible for understanding that all university or auxiliary owned computing devices must be in compliance with university information security standards in order to connect to the network in a Trusted Asset Zone.
- Responsible for understanding that all non-university or non-auxiliary owned computing devices must be granted an exception before connecting to the network in a Trusted Asset Zone.

Non-Compliance and Exceptions:

Systems found in non-compliance with this standard may be removed from the network until they do comply.

If it is technically infeasible for an information resource to meet this standard, departments must submit a request for exception to the VP/CIO and ISO for review and approval.

Related Procedures and Resources:

CSU ITRP Baseline Network Standard Architecture
ITS Firewall Pinhole request process
IP Address Request
Information Security Device Standard