8045.S300 Network Controls Management

Implements:	CSU Policy #8045.0
Policy Reference:	http://www.calstate.edu/icsuam/sections/8000/8045.0.shtml

Introduction

Campuses must establish a method for documenting the campus network topology, equipment configuration and network address assignments.

1.0 Network Information Requirements

Each CSU campus must develop and maintain documentation of its network structure and configuration. At a minimum, the following information must be included:

1.1 Network topology information containing:

a) The locations and IP addresses of all segments, subnets, and VLANs.

b) Identification of any established security zones on the network and devices that control access between them.

c) The locations of every network drop and the associated switch and port on the switch supplying that connection.

d) A summary representation (e.g., drawing) of the logical design appropriate for managerial discussions.

e) A summary security model appropriate for managerial discussion.

1.2 IP address management

a) Static IP address assignments information sufficient to identify host, contact and device location (for wired ports)

b) Dynamic address server (i.e., DHCP) settings showing:

- Range of IP addresses assigned
- Subnet mask, default gateway, DNS server settings, WINS server settings assigned

1.3 Configuration information network devices such as:

a) Switches

b) Routers

c) Firewalls

d) Any other device critical to the functioning of the network

1.4 Configuration information for devices must include but not be limited to:

a) Net masks

b) Default gateway

c) DNS server IP addresses for primary and secondary DNS servers

d) Any relevant WINS server information

e) Responsible administrator contact information

2.0 Network Documentation Management

2.1 Each campus may determine its specific methods for documentation using any combination of online network tools, databases, or hard copies; however, the resulting information must be in a form and format available for audit and review.

2.2 Each campus must establish a method for self-review of network documentation such that each element is reviewed for accuracy and completeness at least every 36 months, and designated critical system information at least every 12 months.

REVISION CONTROL

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
10/8/11	Macklin	Incorporation of ISAC and NTA comments	All
11/9/2011	Moske	Formatted	All
1/11/2012	Macklin	Final review	None
12/13/12	Macklin	ISAC Review – Approved to publish.	Intro
9/26/13	Hendricks	Renumbered for consistency	

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
12/13/12	ISAC	Recommended
6/6/13	ITAC	Reviewed
7/16/13	Perry (CISO)	Approved for Posting