8045.S302 Remote Access to CSU Resources

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

Introduction

Campuses must implement controls designed to protect CSU resources from unauthorized access from external hosts while making these resources available to legitimate CSU users who are not on campus.

1.0 Public Access Systems

Public access systems are those made available to the public via the Internet, requiring no special access or authentication process. Examples include, but are not limited to: campus informational web pages and class schedule information.

2.0 Non-Public Access Systems

Non-public access systems, regardless of where they are hosted, are those that are available only after authentication or other special access process. Examples include, but are not limited to: online courses, class registration web pages, and internal campus email systems

2.1 All remote access (wired or wireless) to non-public campus information assets must:

a) Be authorized and authenticated by use of a unique user identifier.
b) Pass through a campus-approved access control device (e.g., a firewall or access server).
c) Be made using an approved method (e.g. campus-authorized remote desktop service).
d) Use a secure encrypted protocol for the entire session
e) Be logged and tracked consistent with campus logging procedures.

2.2 Non-public access systems must be configured to automatically terminate inactive connections after an appropriate period of time.

3.0 Non-Public CSU-shared Resources

Remote access to non-public CSU-shared resources (e.g., CMS, CSU SharePoint, etc) must, meet or exceed the same access criteria described above for campus information systems and data.

3.1 Campuses must identify and communicate:

a) Approved user practices for remote connections.

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
1/12/2012	Macklin	Format/Bulleting adjustment	All
7/27/2012	Macklin	Clarified definition remote access compromise	
12/13/2012	Macklin	ISAC: non-public systems may be hosted, CSU shared resources minimum and defn language updated. Reporting of device loss removed as it is covered elsewhere. Approved to publish.	

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
12/13/12	ISAC	Recommended
6/5/13	ITAC	Review
7/16/13	Perry (CISO)	Approved for posting