8050.S100 Configuration Management – Common Workstation Standard

Implements:	CSU Policy #8050.0
Policy Reference:	http://www.calstate.edu/icsuam/sections/8000/8050.0.shtml

Introduction

Campuses must develop and implement configuration management standards to address information security risks on campus desktop and laptop computers (workstations) along with associated devices which may store data. Other configuration standards include:

- 8050.S200 Configuration Management – High Risk Workstation Standard
- 8050.S300 Configuration Management – Mobile Device Standard
- 8050.s400 Configuration Management – Common Servers Standard
- 8050.S500 Configuration Management – High Risk Server Standard

1.0 Minimum Configuration Features

1.1 Password Management

State owned desktop and laptop computers must comply with the campus password complexity and aging policies.[1]

1.2 Inventory

a) Campus methods for managing computer inventory must have capability of maintaining inventory records for any campus computing devices, such as workstations, laptops, etc.

b) All desktop and laptop computers purchased by the University must be tracked via the campus inventory management system.

c) The campus must establish a periodic inventory process sufficient to ensure that inventory records are current and accurate, and contain information sufficient to support data classification and incident response activities.

d) All devices, including workstations, peripherals, external drives and memory sticks, which store Level 1 protected data must:

i) Be encrypted using campus approved encryption methods.

ii) Be tracked and managed via the campus inventory process[2].

1.3 Anti-Virus

[1] Please note CSU Standard 8020.S001 Exception Standard for information to be used for any non-compliant workstation.

[2] See also CSU Standard 8065.S001 Information Security Asset Management § 12.4 (http://www.calstate.edu/icsuam/sections/8000/8065.S001_Information%20Security_Asset_Management.pdf)

Up to date anti-virus software must be installed and maintained on all systems. Regular updates to virus definitions and software must be activated.

1.4 Software Updates

Workstation computers must be configured to allow automatic application of software updates through a patch management system.

1.5 Supported Operating Systems

The desktop or laptop device must use a supported operating system in order to ensure that security vulnerabilities are addressed. Where the campus determines that an exception to this standard applies, the campus exception documentation must include controls sufficient to address the risk.

1.6 Enterprise Management

The workstation must be managed by an appropriate configuration management system, such as a campus enterprise desktop management system, that ensures:

a) The workstation is subject to periodic vulnerability reporting.

b) The success and/or failure of critical patches is reported.

1.7 Inactivity Screen Lock

a) Workstations must be configured with screen locking features to prevent unauthorized access to a machine while not in use.

b) Campuses must identify screen lock time limits appropriate to the purpose of the workstation and the environment in which it is located.

REVISION CONTROL

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
0.5	6/10/2014	Macklin	First draft – ISAC development team	All
0.6	6/27/14	Macklin	ISAC dev team review	All
0.7	7/22/14	Macklin	Added	1.8
0.9	9/14/14	Macklin	Revised per ISAC review	All
1.0	10/15/14	Macklin	Incorporated campus feedback	§ 1.2(a)
1.1	5/15/15	Macklin	Incorporated feedback from FOA	§ 1.2(b)
1.2	6/9/15	Grayson	Incorporated feedback from Kircher	§ 1.2(b) § 1.2(c) § 1.2(d) 1.4 1.6
1.3	6/17/15	Grayson	Incorporated feedback from Kircher. Cosmetic	§ 1.2(a)

			changes only.	§ 1.2(b)

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
06/03/15	Perry (CISO)	Reviewed: Submitted to ITAC/ISAC Review Timeframe:06/09/15 until 07/09/15
7/13/15	Perry (CISO)	Approved for Posting