8050.S200 Configuration Management – High-Risk/Critical Workstation Standard

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

Introduction

This standard is intended to provide minimum requirements campuses must implement in order to ensure that those workstations which store or are used to access critical data are protected from unauthorized access.

Other configuration standards include:

- 8050.S100 Configuration Management – Common 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 Definitions

A "High Risk" workstation is defined as any workstation that stores or accesses "critical" data or systems.

"Critical data" includes protected level 1 information in such quantities as to require notification of a government entity (i.e. over 500 records under HIPAA or CA 1798.29), or information classified as protected level 1 due to severe risk[1].

"Access to critical systems" means an elevated access privilege[2] to a system which stores protected level 1 information. Examples of this may include access to the Student Health System, access to payment card processing system, access to student financial records, etc.

2.0 High Risk Workstation Governance

2.1 Incorporating Common Workstation Standards

All High Risk Workstations must meet Common Workstation Standards 8050.S100.

[1] See 8065.S02 Information Security Data Classification
http://calstate.edu/icsuam/sections/8000/8065_FINAL_DRAFT_Data_Classification_CW_V4.pdf

[2] System support personnel with elevated access required to support campus critical systems or infrastructure may need to utilize the campus Exception process as per the CSU Information Security Risk Mangement – Exception Standard 8020.S000.

2.2 High Risk Workstation Designation

Campuses must implement a process for designating and reviewing the designation of critical or high risk workstations.

2.3 Change Control

The configuration of a High Risk Workstation may not be altered except as approved via the campus Change Control Process.[3]

2.4 Physical Security

High Risk workstations must be physically protected as per the as per the CSU Information Security Standard 8080.S01[4].

3.0 High Risk Workstation Configuration

3.1 Network Protection

In order to protect the high risk workstation from malware and/or data exfiltration, network access must be limited. Additional network protection can be achieved by one or more of the following methods, to be determined by risk assessment:

a) Network traffic limited to the minimum necessary to perform business functions by use of isolated network segment with traffic restricted to authorized inbound and outbound ports and destinations. (Please note that this may be used in combination with a virtual desktop environment for other work functions (web browsing, etc.) in order to address productivity.)
b) Intrusion detection and prevention technologies which address hostile sites, malware, etc.
c) Software defined networking, user based and/or application-defined routing or similar use of technology to control connectivity.

3.2 Protection against "zero day" malware

For high risk workstations with operating systems commonly vulnerable to malware, either restricted outbound network egress (see § 3.2(a)) or application whitelisting must be used in order to protect against "zero-day" malware.

3.3 Host-based Firewall

In order to prevent unauthorized access from other "local" hosts, a Host-Based Firewall must be enabled and configured to restrict access to only authorized hosts.

3.4 Security Event Logging

a) The High Risk Workstation must be configured to log security events:

[3] See CSU Information Security Policy: 8055 Change Control along with associated standard 8055.S001 Change Control Standard

[4] http://www.calstate.edu/icsuam/sections/8000/8080_FINAL_DRAFT_IS_Standard_Physical_Environmental_Security_CW_V5.pdf

b) Campus must identity the logging requirements and configuration settings for the high risk workstation and its application environment including:
    i. Remote or local log storage
    ii. Log retention of at minimum 30 days
c) Log activity must comply with 8045.S600 Logging Elements[5]

3.5 Administrative Accounts

Local administration rights must not be granted to the campus account used for activities such as web browsing. As necessary, the user may be issued a separate local administration account.

3.6 Encryption

High Risk Workstations must use University approved encryption on both the hard drive and removable device peripherals and/or media.

3.7 Remote Support

Remote support applications must be configured to require the user to acknowledge and consent to the remote session.

3.8 High Security Workstation Configuration Checklists

High Risk Workstations must use a current standard secure configuration checklist. Useful resources for developing a checklist include but are not limited to those offered by CIS benchmarks, National Institute of Standards and Technology (NIST USCGB) and/or the Department of Homeland Security. [6]

3.9 Vulnerability Scanning

Periodic vulnerability scans must be completed and assessed in order to verify that operating systems and application are adequately updated (see 8050.S100 Configuration Management § 1.4).

3.10 Peripheral Communications

Peripherals and association communication protocols (e.g. Bluetooth) must either be adequately secured via encryption or disabled in order to avoid unauthorized access and denial of service issues.

REVISION CONTROL

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
0.1	6/23/2014	Macklin	First draft – ISAC development team	All
0.4	7/22/14	Macklin	After 7/8 ISAC	

[5] See http://www.calstate.edu/icsuam/sections/8000/8045.S600_Logging_Elements.pdf
[6] http://web.nvd.nist.gov/view/ncp/repository (link to it - add to sound business practices.

0.7	9/9/14	Macklin	After 8/26 ISAC Standard Team review	All
0.8	9/9/14	Macklin	Working on… 9.9 meeting	
0.9	9/14/14	Macklin	Changes accepted – publish for ISAC	§ 3.2 and wordsmithing
1.0	9/23/14	Macklin	Incorporated ISAC comments	§ 3.2
1.1	10/14/14	Macklin	Incorporated campus feedback	§ 2.4
1.2	2/24/15	Macklin	Incorporate CISO comment	§ 3.3

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
11/7/14	ISAC	ISAC approved, moved to CISO review
3/2/15	CISO	CISO Reviewed. Next step is collaborative review.
6/4/15	Perry (CISO)	Approved for Posting