Minimum Desktop Security Standard

Effective Date: July 28, 2015

1.0 INTRODUCTION

California State University, Chico maintains numerous critical assets in the form of confidential data and mission critical systems that all require some level of protection. Security standards for desktops and portable computers are necessary to ensure the availability, confidentiality, and integrity of critical assets maintained by the University. This document is intended to provide a minimum-security standard and a set of guidelines for the installation and support of desktops and portable computers that are part of the CSU Chico network.

2.0 SCOPE

This standard applies to:

- CSU Chico Users: All employees, faculty, staff and third parties including vendors contractors, visitors and all others who utilize the electronic information resources of the CSU Chico System.
- CSU Chico Information Computing Resources: All desktops, laptops, [portable devices], and system software (both first and third party) that are owned by CSU Chico or used by CSU Chico systems.
- Additional standards are required for systems with access to Level 1 data.

3.0 MINIMUM DESKTOP STANDARDS

3.1 Password Management

State owned desktops and portable computers must comply with the campus password complexity and aging policies.

3.2 Inventory

The University approved dynamic hardware and software inventory agent must be used to track all university desktops and portable computers. All desktops and portable computers purchased by the University must have a State ID property tag. All devices (including but not limited to workstations, desktops, external drives and memory sticks) which store Level 1 protected data must be marked with an appropriate State ID property tag. Changes to the campus inventory must be kept current.

3.3 University Approved Anti-Virus

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

3.4 Software Updates Enabled

Desktops and portable computers must be set to allow automatic updates and patching. Operating system updates, application patches and firmware updates should all be included in the scope of the updates.

3.5 University Approved Personally Identifiable Information (PII) Discovery Tool Management

A University approved tool to locate PII (defined by the CSU as Level 1 data) must be installed and run at an interval defined by the University. This will serve as verification that Personal Identifiable Information (PII) is not being stored on desktops or portable computers.

3.6 Green Technology Power Management

Computer equipment is a major consumer of power. Power management needs to be in place to support University sustainability goals. Campus desktops and portable computers must be connected to the campus power management system in order to reduce power. This also allows the ability to shut off power to systems in case of an emergency.

3.7 Vendor Supported Operating Systems

State owned desktops and portable computers should use vendor supported operating systems which continue to deliver security patches. State owned desktops and laptops which utilize unsupported operating systems may not be supported by campus services and may be denied access to campus networks.

4.0 RECOMMENDED BEST PRACTICES (REQUIRED FOR HIGH RISK SYSTEMS)

4.1 Host-Based Firewall

Enabling a host based firewall is recommended to protect individual systems on the network from other possibly compromised systems on the network. Desktops and portable devices should use the software that comes with the operating system or any other third party software approved by the Information Security Office.

4.2 Physical Security

Attention should be given to the physical security of devices, especially those storing Level 1 protected data. Portable devices such as laptops and mobile devices are particularly vulnerable to theft and loss.

4.3 Inactivity Screen Lock

Screen locking features should be enabled to prevent unauthorized access to a machine while not in use. Any exceptions such as public terminals, kiosks, or lab computers should be documented.

4.4 Disable Unnecessary Services

Many systems allow remote desktop protocols to permit access to the system via a different computer on the network. These protocols should be reviewed and only after a justification for need should they be enabled.

4.5 Limit Administrative Account Privileges

At times, users may be granted elevated privileges on a particular system. These privileges should be reviewed and set for specific tasks and not for general work activities.

4.6 Encryption

University approved encryption is required for desktops, portable computers and external hard drives/portable devices storing Level 1 data.

4.7 Remote Support

University approved remote support should be provided to provide support efficiency**.**

4.8 Third Party Application Patching/Updates

Third party applications like Java and Adobe Acrobat are often found to have critical vulnerabilities. It is recommended that all third party applications on desktops and other computing devices are updated and patched when patches become available.

4.9 Application White Listing

Application white listing is a tool that requires approval from a third party/desktop administrator before an unknown and potentially harmful application is installed on to the desktop. The campus currently supports the usage of Bit9 application white listing.

4.10 High Security Workstation Configuration Checklists

The National Institute of Standards and Technology (NIST) and the Department of Homeland Security provide secure configuration checklists which should be used in the configuration of hightg risk systems. http://web.nvd.nist.gov/view/ncp/repository

5.0 ENFORCEMENT

Desktop systems that are not compliant with campus security standards may be denied access to the campus network or otherwise quarantined, either through Network Access Control (NAC) or through additional detection methods.

6.0 DEFINITIONS

System Center Configuration Manager – A systems management software product by Microsoft for managing large groups of computers running Windows, Windows Embedded, Mac OS X, Linux or UNIX, as well as various mobile operating systems such as Windows Phone, Symbian, iOS and Android.[1] Configuration Manager provides remote control, patch management, software distribution, operating system deployment, network access protection and hardware and software inventory.

Personal Identifiable Information – Information that can be used to identify, contact or locate an individual or to identify a person in a single context. This is defined as level 1 data both by the CSU and California State University, Chico.

High Risk Systems – Desktops that regularly store, process or transmit data Level 1 Data.

7.0 REFERENCES

8.0 DOCUMENTATION REVIEW AND APPROVAL

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)	Version
10/3/13	System Security Meeting	Reviewed	V1.0
10/11/13	University Technology Advisory Committee (UTAC)	Reviewed	V1.0
10/22/13	CAD	Reviewed	V1.0
11/18/13	Extended Cabinet	Reviewed	V1.0
04/13/15	Policies and Standards Group	Reviewed / Recommended	V2.0
07/21/15	Information Technology Executive Committee (ITEC)	Approved	V2.0