Securing Critical and High-Risk Workstations Procedure				
	Procedure No	ITS-2020-P	Rev	Interim
	Owner	IT Security and Compliance		
	Approved by	Sheryl Okuno, Director IT Security and Compliance		
	Issued	3-31-2021	Revised	--
				Page 1 of 7

Table of Contents

Contents

1. Introduction and Purpose

Accessing and using Level 1 data to conduct business requirements of the University poses a risk when not appropriately secured. This includes storing, processing, transmitting, and accessing this type of data through unsecured means. This procedure defines the responsibilities and implement controls to identify these workstations to mitigate risks to the University.

CSU Information Security Policy (Section 8050.0, Configuration Management) requires that campuses must implement a process for designating and reviewing the designation of critical or high-risk workstations and that these workstations have:

- Network protection
- Anti-malware protection against "zero-day"
- Host-based firewalls
- Security event logging
- Limited local administrative accounts
- Encryption
- Properly configured remote support applications
- Workstation image meets high security configuration requirements
- Periodic vulnerability scanning

It is the intent of California State University, Los Angeles (Cal State LA) to ensure that workstations used to access Level 1 data, noted as High Risk Workstations, are identified and inventoried and that these workstations meet CSU security and audit requirements.

2. Related California State University Policies and Standards

The following documents of the latest issue in effect represent the criteria against which University information security audits shall be based and shall apply to the extent specified herein. Standards provide detailed supporting and compliance information for policies.

ID/Control #	Description	Title
ICSUAM 8045.S400	*Standard*	*Mobile Device Management*
ICSUAM 8050.0	**Policy**	**Configuration Management**
ICSUAM 8050.S200	*Standard*	*Configuration Management – High-Risk/Critical Workstation Standard*

ICSUAM 8060.0	**Policy**	**Access Control**
ICSUAM 8065.0	**Policy**	**Information Asset Management**
ICSUAM 8105.0	**Policy**	**Responsible Use Policy**
ICSUAM 8050.S200	*Standard*	*Configuration Management – High-Risk/Critical Workstation Standard*
ICSUAM 8045.S600	*Standard*	*Logging Elements*
ICSUAM 8065.S02	*Standard*	*Information Security Data Classification*
ITS-2006-S	*Standard*	*Information Classification, Handling and Disposal*

In support of the CSU policies and standards, the University publishes **standards** (define the minimum requirements necessary to meet CSU policy) and **user guidelines** (provide general recommendations and instructions for users to comply with the policy). These supporting documents are available on the IT Security website under the policy title noted above.

3. Responsibilities

Responsibilities are shared by the academic and administrative departments, data owners/users, data owner department managers, IT Security and Compliance, and IT Infrastructure Services.

3.1 Director, IT Security and Compliance

The director may designate these tasks to staff within IT Security and Compliance as appropriate.

- Interprets and administers the CSU Information Security Policy as it affects workstations and critical workstations.
- Determines appropriate compliance steps and develops procedures necessary to identify and manage workstation risks.
- Maintains standards for information classification.

- Manages security team that monitors vulnerability scanning of identified critical and high-risk workstations.
- Chairs regularly scheduled vulnerability management meetings consisting of ITS managers, asset owners, and system administrators to review vulnerabilities and define remediation efforts.
- Coordinates monthly data inventory scans of workstations using appropriate tools (e.g., Spirion, Microsoft DLP).
- Review monthly data inventory scans to identify high risk workstations with high levels of Levels 1 and 2 data as defined in data classification standards.
- Identifies data owners and workstation hostnames that contain high levels of Level 1 and 2 information.
- Communicates with data owners to ensure they securely clean up unnecessary files or secure required files.
- Assists high risk data owners with use of tools to run data inventory tools to assess storage devices.
- Works with support staff on use of data inventory tools so they can assist users to run searches on their own.
- Works with IT Infrastructure to define and set system policies to ensure critical and high-risk workstations are secured.
- Coordinates with IT Infrastructure to provide data inventory reports so they can implement changes to baseline images to enable that disk encryption, event logging and host-based firewalls on high risk and critical workstations.

3.2 Director, IT Infrastructure Services

- Collaborates with IT Security and Compliance to define and set system policies to ensure high risk workstations are secured.
- Reviews weekly vulnerability reports.
  - Directs the ITS technical remediation efforts because of detected vulnerabilities.
- Reviews high risk workstation reporting from IT Security and manages assignment to team for implementing security policies on high risk workstations.
- Manages the technical implementation of setting policies on baseline images to ensure data encryption, event logging, and host-based firewalls are enabled on high risk and critical workstations.

3.3 Associate Director, IT Infrastructure Services

- Manages the implementation of global policies within the Active Directory environment.
- Enable Azure policies required to support security settings.

3.4 Assistant Director, Desktop Services

- Manages Desktop Services team to implement security policies on baseline images in preparation for deployment on identified critical and high-risk workstations.
- Reviews weekly workstation vulnerability reports to coordinate and address remediation efforts by Desktop Services team on workstation images.
- Manages the security policy settings so that they meet the CSU ICSUAM standard for Configuration Management – High-Risk/Critical Workstations.
- Manages deployment of security policies on workstations identified as critical or high-risk to the business of the University.

3.5 Department Managers

- Identify critical and high-risk workstations and notify IT Security and Compliance so that the critical and high-risk workstation security policy can be applied to the computer.
- Ensure department employees complete data security awareness training.
- Ensures department employees understand their responsibilities for securing sensitive information.

3.6 Data Owners and Workstation Users

- Secures all Level 1 and 2 data when used or stored.
- Locks workstation screen when not in use.
- Maintains secured backups.
- Is aware that they should store minimal sensitive data and only when necessary.
- Reviews monthly data inventory scans to secure information.
- Chooses to store sensitive information on secured servers rather than on workstations or external storage devices that can be lost or stolen.
    - If the need requires local storage of sensitive information data owner must secure the data through encryption.
- When transmitting sensitive information, data owner uses secure transport to ensure data is encrypted when traversing the network.
- Knows where sensitive data is stored.

- Ensures that workstations used remotely, connect to the campus network via VPN or bring equipment onsite for baseline image patches and updates that must occur monthly.
- Uses complex passwords.
- Uses 2-Step Verification (MFA) to secure access and credentials.
- Shares sensitive data only for specific university business and only when data is encrypted.
- Has the capability of running data inventory tools (included with baseline image) periodically as needed to identify Level 1 and 2 data stores.
- Collaborates and works with ITC and ITS to secure Level 1 and 2 data.
- Completes periodic data security awareness training.
- Contacts IT Security and Compliance immediately when workstation or storage devices are lost or stolen.
- Ensures the physical security of university equipment at all times.

3.7 Information Technology Consultant (ITC)

- Provide direct support to departmental users with workstations storing and accessing Level 1 and Level 2 data.
- Works together with ITS to ensure department employees review their monthly data inventory scans to identify and tag false positives as well as secure necessary files and securely delete files no longer needed.
- Alert the Director, IT Security and Compliance when ITC identifies critical or high-risk workstations.

4. Procedures

4.1 Conduct Data Inventory

Each month, the IT Security and Compliance department runs an automated data inventory scan of data stores. The data collected feeds into a dashboard showing user IDs, departments, divisions, hostnames, the amount of Level 1 data tags identified, and if the user has reviewed the data to check for false positives, encrypt data or securely delete unnecessary data.

4.2 Classify Data, Identify Data Owners and Critical/High-Risk workstations

IT Security and Compliance reviews the monthly data inventory scans and contact users when the dashboard information shows high levels of Level 1 data tags that have not been reviewed

by the user. If there is no response from the user, IT Security and Compliance will work with the department and their ITC to locate the workstation, communicate with the workstation user or the department manager and assist the user with the review. Non-compliance to review and secure the information will automatically be recorded as a high-risk workstation and a ServiceNow ticket will be opened to apply the critical/high-risk workstation policy to the workstation.

Departments and ITCs also must collaborate with ITS when they identify critical workstations used to access and process Level 1 and 2 data so that proper security controls are put in place. A ServiceNow ticket will be opened by the department ITC to request the critical/high-risk workstation policy be applied to the workstation.

4.3 Departments Managers and Data Owners

After each monthly data inventory scan completes, Data Owners must review the data scan results. Any data stores identified incorrectly (e.g., 9-digit Campus ID Numbers that look like social security numbers) must be marked as “Ignore” with a notation of “False Positive”. For all other files containing sensitive and Level 1 information, the workstation user must secure the file or securely delete the file using the data inventory tool.

4.4 Securing Critical and High-Risk Workstation

When a ServiceNow ticket has been opened, the ticket will be assigned to the IT Infrastructure Desktop team. The desktop team will apply the critical and high-risk workstation policy to the workstation.