Workstation Encryption

PURPOSE:

This Business Practice establishes the requirement and process for encrypting workstations at CSUCI. The purpose is to reduce the risk of sensitive data exposure through the loss or theft of devices. Encryption is a critical safeguard against security breaches that could result in violation of legal statutes, financial penalties, reputational harm, and loss of public trust.

Scope:

This practice applies to all University-owned and -managed workstations, including desktops, laptops, and tablets, that are used by faculty, staff, auxiliaries, and contractors.

Policy Statement:

1. All workstations that process or store Level 1 or Level 2 sensitive data (confidential or internal use) must be encrypted.
2. As a general practice, all University-provided and maintained workstations will be delivered and managed by ITS in an encrypted state, regardless of whether sensitive data is anticipated to be stored.
3. Any user or group requesting to operate a university managed workstation without encryption must obtain an exemption from the Chief Information Security Officer (CISO). Exemptions will only be considered when:
    a. The device does not contain or process sensitive data.
    b. The requesting unit demonstrates a valid operational need for non-encryption.

Definitions:

Encryption: The process of encoding information to prevent access by unauthorized parties. For CSUCI workstations, full-disk encryption (e.g., BitLocker for Windows, FileVault for macOS) is the standard.

Sensitive Data: Information classified as Level 1 (Confidential) or Level 2 (Internal Use) according to CSU data classification standards.

Roles & Resposibilities:

- **ITS User Services (Workstation Administrator)**
  - Deploys all University workstations with full-disk encryption enabled.
  - Maintains central management of encryption keys and compliance status
- **Information Security (ISO)**
  - Ensures compliance with CSU and CSUCI security standards
  - Reviews exemption requests and makes recommendations to the CISO
  - Monitors encryption compliance through periodic assessments
- **Chief Information Security Officer (CISO)**
  - Reviews and approves or denies requests for exemption from workstation encryption
  - Maintains records of approved exemptions
- **Users/Departments**
  - Must not attempt to disable encryption on university-managed workstations
  - Responsible for submitting exemption requests if encryption interferes with required work

Process:

Standard Encryption Deployment
- All workstations deployed by ITS will be encrypted prior to delivery.
- Encryption status is verified at setup and monitored periodically by ITS

Exemption Process
- A user or department seeking exemption must submit a request to the CISO through the IT helpdesk
- The request must:
  - Identify the device(s) in question,
  - Provide justification for exemption
  - Confirm that the device will not store or process sensitive data
- The CISO will review the request
- The CISO may grant or deny the exemption. Approved exemptions will be documented

Compliance Assessments
- Information Security will conduct periodic reviews of encryption status across university-managed devices
- Findings will be reported to ITS leadership, and remediation steps will be initiated where required

Enforcement:

Non-compliance with this practice may result in revocation of device access to university systems and networks, and escalation to division leadership

Related Documentation

- CSU Information Security Policy – ICSUAM 8000 series
- CSU Information Security Standard – 8050.S100 Common Workstation Configuration Standard

Contact

Information Security Team – infosec@csuci.edu
ITS Help Desk – helpdesk@csuci.edu

Assessment Requirements

Assessment requirements and history are listed in the grid below

Description	Frequency	Role Assigned
Review business practice	Annual	CISO
Review list of the encrypted and not encrypted devices	Annual	CISO, Director of User Services, Director of Technology Infrastructure

Revision History

BP Number:	BP-05-011	**Date Created:**	10/01/2025	Revised by
Revision Number		**Revision Date**		