Process Number: BP.03.002.04 **Effective Date:** 13-September-2010

Approved By: James August **Page 1 of 5**
AVP for Information Technology Services

Business Practice for Administrative Access to Workstations

PURPOSE:

To assure the confidentiality, integrity, quality, and availability of CSU Channel Islands information assets by limiting administrative access to workstations to those with a legitimate academic or business need for access.

BACKGROUND:

CSU Channel Islands ITS strives to provide a high-quality and feature-rich computing environment. ITS depends upon the standardization of the computing environment to deliver quality service and support to students, staff, and faculty. Internal policies, such as the Interim Policy on Responsible Use (IT.03.001), require ITS to implement processes to ensure the appropriate use of information systems. Additionally, the University is required by CSU system-wide policy to protect its information assets.

As computers and their associated operating systems grow in complexity, they also become more complicated to manage. Most operating systems and software developers have a two-tiered approach to computer access rights, with regular users and administrative users. For most operations, regular user privileges are sufficient to complete work-related tasks and to provide limited customization of the computing environment. By contrast, administrative users are granted full control over the system or service to which the administrative access applies and can make any and all modifications to the machine.

BUSINESS PRACTICE:

Accountability:

Director, User Services.

Applicability:

- All CSUCI users of university-owned or managed computing devices, including workstations, laptops, tablets, and servers.
- All CSUCI users granted administrative or elevated access to such systems.

Definitions:

1. Administrative Access: Privileged access beyond that of a regular, non-administrative user.

2. Administrative User: A user with administrative access to a system or service.

3. Regular User: A user without administrative access to a system or service.

4. Workstation: A University-issued or –owned computer. “Workstation” encompasses any computer issued to or shared by an individual, including desktops, laptops, and tablets.

5. Server: A physical or virtual system that provides centralized computing services, applications, storage, authentication, or other infrastructure functions to multiple users or systems.

6. Server Administrative Access: Elevated access rights (including root, local administrator, domain administrator, service account control, or equivalent privileges) that permit configuration changes, software installation, service management, or security modification on a server.

7. Server Administrative User: A user granted Server Administrative Access.

Detail

In order to ensure the confidentiality, integrity, and availability of the University’s information assets, ITS will implement the following procedures.

Administrative access to workstations — General

CSUCI ITS operates on the assumption that faculty and staff are granted regular user access to their workstations and provides a standardized computing environment to support their work. Limiting administrative access helps maintain system integrity and simplifies troubleshooting, centralized management, and system upgrades. The CSU discourages faculty and staff from having administrative access to their machines.

In accordance with CSU Information Security policies (.pdf), "ISO Domain 9: Access Control", all changes to a computer must follow an approved request process, and local administrative rights must not be granted to accounts used for activities such as web browsing. This means that users requesting administrative access will be issued a separate account for only that purpose.

CSUCI must ensure that all computers:

- Use a current, standard, secure configuration
- Have up-to-date anti-virus software with automatic updates enabled
- Receive automatic software updates through an approved patch management system

- Use a campus-approved image; reformatting is not allowed

Users with administrative rights must not disable or modify any services that support malware protection or routine maintenance.

Users granted administrative access are responsible for the administration of their workstations and must comply with the Administrative Access Rights Service Level Agreement. Administrative access may be suspended or revoked at the discretion of the AVP for Information Technology Services if sufficient system administration skills are not demonstrated.

Administrative access to workstations for Staff (including student employees)

CSUCI ITS restricts administrative access to staff member workstations to those who have a demonstrated business need for access to those workstations.

For a staff member to gain administrative access to their workstation, that staff member must—

- Have a demonstrated business need for administrative access to their workstation(s). Installing software on university computers is not sufficient business justification.
- Obtain the verification of a demonstrable business need from their program or department manager,
- Obtain approval from their division executive (see Exhibit 2),
- Obtain approval from AVP for Information Technology Services, and
- Complete and agree to the Administrative Access Rights Service Level Agreement (see Exhibit 1).

Administrative access to workstations for Faculty

CSUCI ITS may provide faculty members with administrative access to support the academic mission of the institution. The AVP for Information Technology services will approve access for faculty who have a clear need that cannot otherwise be met by ITS (i.e. operating scientific equipment, programming, research, or teaching classes that would be hindered by a lack of administrative access). Requests that are not clear (user requesting administrative access for routine software installation) will be escalated to the appropriate Dean for approval and risk acceptance.

Administrative access to workstations — Students

Student employees must comply with the processes for staff members above.

Providing administrative access to workstations to non-employee students is prohibited unless those workstations are physically isolated from the campus production network.

Administrative access to servers — General

CSUCI ITS manages campus servers as shared enterprise resources that support the University's academic and business operations. Because servers typically host multi-user services, institutional data, authentication services, research systems, or mission-critical applications, administrative access to servers presents significantly greater institutional risk than workstation administrative access.

Administrative access to servers will be limited to individuals with a documented operational, academic, or business need.

All campus servers must:

- Be deployed using an approved, secure baseline configuration
- Participate in centralized patch management
- Run campus-approved endpoint protection and monitoring tools
- Be enrolled in centralized logging and security monitoring where applicable
- Not be reconfigured in a manner that disables required security controls

Server administrative users must not block, disable, or alter required security configurations, monitoring agents, vulnerability scanning tools, or patch management services.

Administrative access to servers — Responsibilities

Users granted administrative access to servers bear heightened responsibility for safeguarding institutional systems and data.

Server Administrative Users must:

- Install and maintain only applications, services, and components required to support documented academic or business functions.
- Do not install software for convenience, experimentation, personal productivity, or other non-business purposes.
- Ensure all installed software is vendor-supported, actively maintained, and kept current with security updates.
- Remove software that is outdated, unsupported, no longer required, or introduces security risk.
- Do not run development, testing, or experimental software on production servers unless explicitly authorized.
- Configure servers according to the principle of least functionality to minimize exposed services and reduce attack surface.

Installation of unauthorized, unsupported, or unpatched applications on university servers may result in immediate suspension of administrative privileges and removal of the system from the production network.

Administrative access to servers — Approval Process

Administrative access to servers requires:

- A documented business or academic justification,
- Approval from the system owner or department head,
- Approval from the AVP for Information Technology Services or designee,
- Completion of a Server Administrative Access Service Level Agreement.

Access will be reviewed annually and revoked when no longer required.

Exhibits:

The following document is incorporated by reference. Please consult https://www.csuci.edu/its/policy/ *for details.*

Exhibit 1 - Administrative Access Rights Workstations Service Level Agreement (Reference)
Exhibit 2 – Administrative Access to Workstations – Business Justification and Approval (Reference)

Assessment Requirements

Assessment requirements and history are listed in the grid below.

Description	Frequency	Role Assigned	Date Completed
Annual review of this practice	Annual – July	Director, User Services	06/09/2026

Revision History

BP Nbr:	BP-03-002	**Enacted Date:**	09/13/2010

Revision Nbr:	001	**Revision Date:**	08/12/2013	**Revised By:**	Neal Fisch
	002		02/02/2017		NFisch
	003		01/03/2024		C Miranda
	004		06/09/2026		J August