Administrative Privileges

Overview
Campus Computing provisions user accounts with the least privilege required to perform typical or everyday computing tasks. The least privilege, in most cases, is all that is needed by employees to perform their assigned job duties. Campus Computing employees and some other USFSP employees may require higher levels of access (or administrative privileges) on USFSP technology resources. Additional standards and procedures are in place to ensure the security, integrity, uninterrupted operation, and prevention of unauthorized access to technology resources for users given access to user accounts with administrative privileges.

Purpose
The purpose of this document is to establish the rules for the creation, use, monitoring, control, and removal of user accounts with administrative privileges on USFSP devices.

Scope
This policy is in effect for all USFSP employees that have, or may require, administrative privileges on any USFSP technology resource.

Definitions
The following terms may be used within this policy or on related documents:

- **Administrative privileges** provide user accounts with a higher level of access than that of a regular user account. These privileges allow user accounts to perform additional system administration tasks such as installing software and making system configuration changes.
- **A local user account** is an account that lets you sign in to only one device. Local user accounts must be provisioned on each device by a user account with administrative privileges.
- **A domain user account** is an account that lets you sign in to multiple devices connected to a domain. At USFSP, our domain user accounts are known as Bayboro Accounts. The first time a user signs in to a device with a Bayboro account the device must be plugged into the wired Bayboro network.
- **Institutional data** is defined as all data elements created, maintained, received, or transmitted as a result of business, educational or research activities of a USF System unit and may include one or more of the characteristics listed in USF System Policy 0-507.
- **USFSP technology resources** shall be interpreted to include all USF System computing and telecommunications facilities, equipment, hardware, software, data, systems, networks, and services which are used for the support of teaching, research, and administrative activities of the USF System.
Policy
- User accounts with administrative privileges are NOT to be used to perform typical or everyday computing tasks. These accounts are for performing device management responsibilities only.
- An additional user account will be created (by Campus Computing) on each device that will be used to perform device management responsibilities. In most cases, this user account will be a local user account.
- Employees outside of Campus Computing are NOT permitted to create or modify administrative accounts.
- The password for each administrative user account must comply with the requirements within the USF System Technology Procedure: Choosing Strong Passwords (ISSP-005).
- Administrative user accounts must NEVER be shared between users.
- Employees with administrative privileges are responsible for understanding and complying with USFSP CCS Standard: Appropriate Use of Administrative Privileges.

Enforcement
Violation of this policy will result in administrative privileges being revoked. Please see USFSP CCS Standard: Appropriate Use of Administrative Privileges for inappropriate uses of administrative privileges that will result in a violation of this policy.

Administrative Privileges Request Procedure
Employees that need to perform device management (or system administration) tasks on university devices can request administrative privileges by completing and submitting the USFSP CCS Local Administrative Privileges Request Questionnaire. Not all exception requests will be approved.

Related Documents
- USFSP CCS Standard: Appropriate Use of Administrative Privileges
- USFSP CCS Local Administrative Privileges Request Questionnaire
- USF System Technology Policy: Using and Protecting Microcomputing Resources (0-501)
- USF System Technology Policy: Appropriate Use of Information Technology Resources (0-502)
- USF System Technology Procedure: Choosing Strong Passwords (ISSP-005)
- USF System Technology Standard: Securing Sensitive Computers (ISSP-006)
- USFS System Technology Standard: Data Protection for Mobile Devices (ISSP-012)