Assigned Administrative Privileges Standards

Standards Information

Date Adopted
…
Implementation Date
…
Revision Date
…
Next Review Date
…
Responsible Office
Information Technology, Information Security Office

Background

Administrative Privileges on computer devices are typically reserved for an organization's IT staff who are responsible for computer systems management and user support. This is because administrative privileges allow a user to perform actions which can negatively impact the security, stability, and usability of the computer, other UM computer systems, and the UM data network. UM IT needs to ensure a high level of security, stability, and usability for our computer environment by limiting the use of administrative privileges to those users who have demonstrated a need, acknowledged the responsibilities associated with administrative privileges access, and obtained supervisor and Dean/VP or designee approval.

However, using administrative access for everyday tasks such as reading email or browsing the web carries an increased risk. Malicious software can take advantage of administrative privileges to jeopardize the operational integrity of a computer system. Compromised accounts with administrative privileges may allow intruders to disrupt UM's computer or network operations; steal information; or allow unauthorized access to data residing on the system or attached devices. Improperly applied administrative privileges may directly impact the availability of both computing resources and IT professional support. For this reason, it is prudent to restrict administrative access to those who truly need it for academic or business needs.

Routine tasks that do not require administrative access, such as web browsing and reading of email, should be executed using unprivileged accounts. Administrative privileges should be granted under the IT concept of "least privilege", meaning elevated privileges should only be granted to end-users who have a legitimate need. Tasks should be performed using the most appropriate privilege level.

Definitions

- Assigned Administrative Privileges – Access level that allows an individual unrestricted access to change the configuration of operating system level settings on a specific desktop, laptop, virtualized system, or server.
- Least Privilege – The minimum resources required for a user to perform their official job functions.

Purpose

The Assigned Administrative Privileges Standards has been established to define the criteria for which Administrative Privileges for a UM-owned and UM IT supported computer may be granted, and the terms and conditions upon which rights may be granted.

UM IT will grant Assigned Administrative Privileges, as appropriate, to those employees who require such rights to perform their duties. UM IT will strictly adhere to the principle of 'least privilege' when granting rights to UM-owned computers. Rights will only be granted under the condition that they are essential to the performance of the grantee's job. Lack of adherence to all UM and MUS IT policies may cause revocation of these rights. UM IT will manage all accounts that require Assigned Administrative Privileges. Standard procedures will require a recurring review and revalidation of Assigned Administrative Privileges, at least annually, if not specified more frequently by UM IT or the UM Information Security Office. All users requesting Assigned Administrative Privileges rights must complete the following:

- Submit Assigned Administrative Privileges Request Form – TBD (UM IT)
- Enrollment into UM Security Awareness and Training Program – TBD (ISO)
- Acknowledge Assigned Administrative Privileges Responsibilities – TBD (ISO)

If the request for Assigned Administrative Privileges is granted the access control will be created by UM IT staff. This access control may be in the form of a separate username/password credential or may be a tool that temporarily elevates your standard username credentials to an administrative role. Whether this is a separate administrative credential or an elevated standard credentials, this administrative role is to be used only when you need to use administrative rights on your UM-owned computer and only for the specific purpose the administrative rights were granted to you.

Responsibilities

Users who have been granted Assigned Administrative Privileges access on their computer must:

- Not interfere or disable any patching, software updates, malware checking, or security operations
- Purchase or procure all software through UM IT or in consultation with UM IT
- Ensure that all software installed has been reviewed by UM Accessibility

- Never share their username and password credentials with others
- Report system failures and/or security compromises to UM IT Help as soon as possible
- Review and comply with the following policies
    - UM Information Security Policy
    - UM Password Policy
    - UM Data Classification and Handling Policy
    - UM Registration and Protection of Endpoints Policy
- Never use their administrative privileges for non-administrative tasks

Abuse

If a user abuses their Assigned Administrative Privileges, UM will revoke the administrative rights access control.
Abuse is defined as, but not limited to:

- Downloading software that is malicious to the UM network
- Downloading unlicensed or illegal software to UM-owned computers
- Causing a breach of Sensitive Data (Level 3) or Highly Sensitive Data (Level 4) as defined in the Data Classification and Handling Policy