Administrative Privileges Policy

The following document applies to all university employees and computers, including Information Technology Services (ITS) employees and computers.

Running a computer system with administrative privileges represents a significant risk to the confidentiality, integrity, security, and availability of the University's information assets. However, without elevated administrative privileges, a user cannot immediately install or update some software and/or hardware and must wait for ITS support, which causes an inconvenience for the user and increases the expense of maintaining the University's computer assets. Therefore, under the direction of the university administration, ITS enables automated temporary access to elevated administrative privileges for each employee on their assigned computer to perform job-related duties.

All university-owned computers must:

- Be joined to the University's active directory domain;
- Have management software installed that facilitates hardware or software inventory for asset tracking, license compliance, software installation/upgrading, remote assistance, or troubleshooting;
- Have active, properly configured security (anti-virus, malware, etc.) software;
- Have service packs and/or patches deemed necessary by ITS.

NOTE: Exceptions to the above can be made by the Chief Information Officer.

Administrative Privileges Agreement

Every university employee has automated temporary access to elevated administrative privileges for job-related duties on their university-assigned computer and is required to abide by the following:

- Users will not alter the computer's firewall, antivirus, or any other security software;
- Users will not create any new user accounts or modify any existing accounts;
- The ITS department will continue to provide operating system patches, application software patches, antivirus/malware updates through the system wide client management platform to all University owned computers. Users will not block or in any manner disable or revise any services on the computer that may prevent these or other routine maintenance procedures including scheduled antivirus/malware scans;
- Users will maintain software licensing information for any software personally installed on their assigned computer;
- User will not share their username or password with others (ITS can provide assistance in establishing options for securely sharing items between users);
- Users will not install or use software that is considered insecure. If there are questions concerning the validity of any software, the user should contact ITS prior to installing;
- Users agree that ITS has the right to temporarily block the computer from the university network at any time if the computer is suspected to be a security or support risk;
- Users will be responsible for backing up their data. ITS will not be able to restore a configuration

customized by the user. In the event of a computer failure, ITS will restore the original base image on the computer. The base image includes an operating system, and any software maintained by the ITS department;

- Users agree that, in the event their elevated administrative privileges result in a security compromise, they may be held responsible for any damages that may result to the full extent allowed by university policy, local, State, and/or Federal law.

Privileges Revocation

A user's elevated administrative privileges may be revoked for any of the following reasons:

- User is involved in a data breach that is related directly to their having administrative privileges;
- User is downloading or installing software that is illegal or malicious to the University's IT Resources;
- User is downloading or distributing copyrighted material without permission and can't demonstrate "fair use" (http://www.copyright.gov)
- User requires excessive support from ITS staff. Excessive support is defined as frequent incidents requiring ITS staff to spend time returning a computer's operating system or software to a properly functioning state.

Decisions to revoke a user's elevated administrative privileges will be made collaboratively by the Executive Director of ITS and the immediate supervisor of the assigned user based on documentation of any of the above conditions. Revocation of privileges will be communicated in writing to the user upon execution. If the Executive Director and the user's immediate supervisor are unable to reach a mutually acceptable agreement, either may appeal to the Technologies Advisory Committee (TAC) for a decision. The committee may be reached by sending a written request to the TAC Chair. The Chair will respond to appeal requests in writing to the requester within 15 business days. In the meantime, prior to the TAC's official decision, revocation of elevated administrative privileges is at the discretion of the Executive Director.

A user's previously revoked administrative privileges will not be restored without a written request from the user. After a period of 90 days, a user may request the reinstatement of their previously granted elevated administrative privileges by sending a written request to the Executive Director and their immediate supervisor. The decision process will consider the documentation and/or decision that led to the revocation and the user's computer use record during the prior 90 days. If the decision is made to continue without elevated administrative privileges, the user may continue to request reinstatement every 90 days. Any reinstatement request that is less than 90 days from the initial revocation or from a previous reinstatement request will not be accepted.

A user whose administrative privileges are revoked and not restored may appeal the decision with the TAC. The committee may be reached by sending a written request to the Executive Director and the TAC Chair. The committee will respond to appeal requests in writing to the requester within 15 business days.

Approved by the Shared Governance Executive Committee and the President, 02/06/2014.
Approved as modified by the SGEC and the President, 03/15/2021.