LOCAL ADMINISTRATIVE PRIVILEGES AND NETWORK COMPUTER MONITORING 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 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 local administrative privileges for each employee on their assigned computer.

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 Executive Director of ITS.

Local Administrative Privileges Agreement

Every university employee initially has local administrative privileges on their university-assigned computer and is required to abide by the following:

- User will not alter the computer's firewall, antivirus, or any other security software;
- User 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. User 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;
- User will maintain software licensing information for any software personally installed on their assigned computer;
- User will not share their username or password with others (Information Technology Services can provide assistance in establishing options for securely sharing items between users);
- User 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;
- User agrees 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;
- User 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;

- User agrees that, in the event their local 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.

Network and Computer Monitoring

Electronic information on university computing resources is subject to examination if it is necessary to maintain or improve the functioning of university computing resources. Therefore, it is understood that there is a need to periodically inspect computers and network usage in order to ensure the continued correct operation of the university network and computing resources.

The University does not condone censorship, nor does it endorse the routine inspection of electronic files or monitoring of network activities related to individual use. At times, however, legitimate reasons exist for persons other than the account holder to access computers, electronic files, or data related to use of the university network. Such monitoring is limited to the backup, caching of data, logging of general activity, and usage patterns as are necessary for maintaining network availability or performance.

The University may monitor individual usage in the following instances:

- The user has voluntarily made access available to the public;
- To protect the security, functionality, and liability of the University's IT Resources;
- Where probable cause exists to believe that the user has violated this policy.

Any such monitoring of individual activity, with the exception of when a user voluntarily grants access, must be approved in advance by the Vice President of Business and Financial Affairs (VPBFA) in consultation with the President. The University may also monitor individual usage upon receipt of a legally served directive of appropriate law enforcement agencies. In these instances, the user will not be notified, so as to not impede on investigations by proper authorities. The VPBFA must be notified prior to initiation of monitoring.
Any violation of these procedures or unauthorized monitoring by the University will be considered "misuse" and personnel involved will be subject to disciplinary action.

Privileges Revocation

A user's local 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/fls/fl102.html);
- 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 local administrative privileges will be made collaboratively by the Executive Directof 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 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 local 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 local 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 local 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