Administrator Privileges Accountability Statement

General Statement

Administrator privileges allow a user to have full access of a local computer. Administrator privileges may be required to install software and updates, perform computer management tasks, or run certain software packages. Tasks should be performed using the most appropriate privilege level.

The nature of certain functionality\(^1\) in conjunction with the need for expeditious resolution to specific projects and problems has emphasized the need for members of the organization to be able to do certain activities on their local computers that have previously been reserved for system administrators. While it is the preferred method to have Information Technology Services (ITS) make configuration changes or install software in a timely manner, ITS is fully aware that at times that may not be a viable solution. The purpose of this document is to define responsibilities, delegation, support, and potential consequences in the granting of local administrator privileges to individuals.

The overriding intent of this document is to protect university resources (such as data, computer systems, networks, etc.) from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to the university’s public image (i.e. disclosure of alumni personal information).

Responsibility and Support

The responsibility for university-owned machines is a shared responsibility between ITS and the user. ITS is responsible for ensuring the device meets the OSU Minimum Computer Security Standards (MCSS\(^2\)), and if the device is a notebook computer, the hard drive must be encrypted if it contains restricted data\(^3\). These controls are only managed by ITS when the device is connected to the FCOB local area network. The controls, however, will remain in effect when disconnected from the network to provide the device and user a baseline level of security. These controls are requirements and must not be circumvented.

For the user, the assumption of local administrator privileges on a university computer carries certain inherent responsibilities. Care must be taken due to the potential loss of data, compliance with copyright laws and potential threat of compromise. FCOB users who are

\(^1\) Examples: installing applications, installing printer drivers, changing the system time or time zone, installing security patches, and running Windows tasks or administrative tasks.

\(^2\) MCSS requires devices to have an active firewall; operating system and application have current security patches installed; active and current anti-malware protection; and appropriate authentication controls.

\(^3\) Restricted data is data protected or regulated by law or critical to university operations including personal information such as SSN, credit card numbers and trade secrets.
granted administrator privileges should be aware that they would become fully and solely responsible for any data that is stored locally on the computer they are administering, and as such, must:

- Never alter the information security controls established by FCOB ITS. This includes circumventing the local firewall, anti-virus, anti-malware, and software auto-update functionality. Removing or deactivating these safeguards increases the risk of unauthorized access and device compromise.

- Adhere to the software license agreement(s) associated with any software installed on the computer. Users who are granted local administrator privileges should be aware of copyright restrictions and licenses placed on ALL software installed on their systems as well as being aware that there exist severe criminal and civil penalties for noncompliance.

**Password Security**

It is important that accounts with administrator privileges have strong passwords. Administrators should never share their password or account with any other person, for any reason. If they find out their password has been compromised, or their account has been otherwise compromised (even by an editor or individual they know and trust), they should attempt to change it immediately, and report the incident to ITS. ITS will never ask a user for their password.

**Delegation**

The user assigned local administrator privileges, cannot create additional local accounts or delegate administrator privileges. ITS must grant or delegate administrator privileges.

**Standard Non-Compliance**

Failure to comply with the Local Administrator Privilege agreement may result in the suspension of any or all access privileges, disciplinary action, or possible termination of employment.