Columbus State University
Local Admin Security Policy Exception and Agreement

Revised 12/11/2017

1.0 Background

The Local Admin Security Policy states that UITS installs all PCs with **limited local user rights (non-Admin).** However, if the user demonstrates a legitimate need and direct impact on the ability to perform work duties to serve CSU students, the CSU Information Security Officer may approve exception.

2.0 Purpose

The purpose of this policy and agreement is to ensure that users are aware of, and agree to, the responsibility that having elevated local user rights, known as "Local Admin rights" entails. Local Admin rights allow the user to modify the PC on a system level. Furthermore, these rights may cause a PC to be susceptible to the vast array of exploits that exist on the Internet.

3.0 Policy

Any CSU user granted Local Admin rights must accept and adhere to the following:

- The user must not perform any actions through the "admin" account that is in violation of any other CSU policy.
- The "admin" account must be used for CSU authorized business only. Not for personal business.
- The user must log off the computer when it is not in use.
- The computer must employ automatic operating system updates.
- The user must comply to all USG and CSU policies regarding critical student, network, and system confidentiality of Personally Identifiable Information (PII) data.
- Upon approval of Local Admin rights, the user will receive another CSU admin privilege account login "admin specific". Do not use this admin privilege account while working with any student Personally Identifiable Information (PII) data due to the high risk of possible data compromise. Only use your MyCSU account when working with student PII data.
- In the event of computer problems associated with the admin account usage UITS Desktop Support may be required to re-image the PC and give it back to the user with all default settings and software. ***Backup data to H:drive per CSU Computer Use Policy***
- UITS must record the physical location, network address and any other identifying information of the computer for inventory purposes.
- UITS will periodically assess the computer to verify that it is operating under a secure framework and complies with CSU software licensing and other policies.
- UITS will create a local admin account for technicians to utilize. The user may not alter this account in any way.
- If the computer becomes unsecured or compromised in any way (ex. connecting personal hardware, loading unauthorized CSU business software), UITS will disable the computer's network access until remediation is complete and the computer is secure.
- UITS cannot guarantee that remediation efforts will be successful; in that event, the computer will remain disabled until UITS can rebuild it. A service request will be submitted into the normal UITS workflow and will not be given high priority.

Violation of this policy or repeated computer compromises will allow decisions to be made pertaining to the user losing the privilege of Local Admin rights.

By signing below, the user accepts the conditions of this policy. UITS must keep a copy of this form and give a copy to the user.

_____ _____

CSU User Name (Printed) **eQuest #**

_____ _____

CSU User Signature **Date**

_____ _____

Supervisor Signature **Date**