

Columbus State University Local Admin Security Policy

Revised 6/21/2007

1.0 Background

In today's ever-changing computing environment, users have more information at their fingertips than ever before. CSU computers connect directly to the Internet, providing for virtually unlimited informational resources accessible "anytime, anywhere" on campus. With this type of access comes the need for increased security and protection against the vast array of exploits designed to compromise personal computers and indeed entire networks. Spyware, viruses, worms, active-x web based intrusion programs, remote access programs, key loggers, and many other exploits install on a PC without the user's knowledge. Not only can these programs do irreparable harm to a PC, but may also launch network attacks, both on and off campus.

2.0 Purpose

CINS is responsible for the security and proper use of computers connected to the CSU network. Moreover, CSU is liable for any malicious activity or harm caused by a compromised PC on its network. A policy concerning Windows Local Admin permissions is intended as a means to consistently and proactively:

- Reduce lost productivity for the end-user
- Reduce the time spent by CINS technicians on remediation and re-installation of compromised PCs
- Reduce network management and incident response efforts.

3.0 Policy

CINS installs all computers with **limited local user rights (non-Admin)**.

With limited local user rights the user cannot:

- Install software or drivers
- Make system level changes
- Allow malicious programs to install
- Unknowingly allow their system to be compromised

The practice of limiting local user rights protects the user and the PC and helps to ensure optimal performance and reliability.

Since software installs, updates, or system level changes will require the service of a CINS technician, planning is essential on the user's part. CINS places a high priority on requests of this type.

The Information Security Officer may approve exceptions to this Windows Local Admin Security Policy. A legitimate need and direct impact on the ability to instruct students must be demonstrated. In addition, the user must agree in writing to adhere to the Local Admin Security Exception Policy and Agreement.