Scope
This policy applies to the College of Dentistry’s policy on administrator accounts on College of Dentistry computers.

Policy

Local administrator rights on all College of Dentistry computers is restricted. This is implemented for 2 reasons, protection of our patient data (security) and software licensing. For security reasons computers with administrator rights are more susceptible to virus, malware and spyware software being installed. All of the college’s computers access Axium and MiPacs, which contain Protected Health information (PHI), so we have to protect our patient data. Many collegiate computers also have identifiable research data on them which also falls into PHI security rules. With all our patient data now electronic we have to do a better job of securing our computers, infrastructure and data.

All software on College of Dentistry computers must have a valid license. In order to make sure the college is compliant with software licensing, we need to track all software that is licensed and installed. As part of software licensing we will be conducting a software inventory on all computers, checking against current licensing numbers and notifying departments if there are any discrepancies. It is illegal to purchase one copy of a particular software and install it on multiple computers. If you need software installed on your computer contact Technology and Media Services help desk. There must be proof of a valid license before we can install any software. There will be no exceptions to this policy.

Studies from security firms show that some 90% of Windows 7 and 100% of Microsoft Office vulnerabilities reported in 2009 could be avoided if the user did not log in as an administrator. Other software products have similar results.

Frequently asked questions

Q1. My computer does not have axium or any clinical data on it. Does the policy below apply to me?

A. Yes, all managed computers in the college are included in the policy. A managed computer is defined as connected to the campus network, included in the Iowa domain, and authenticated to with a hawkid and password.
Computers without clinical data are just as susceptible to attacks and being compromised. Depending on the type of threat, a compromised computer may try to infect other computers on the same network, which means an infected nonclinical computer could infect a clinical computer. With that in mind we need to treat all managed computers the same.

Q2. What about laptops?

A. Most of the college’s laptops are managed and included in the above policy. People using a managed laptop as their primary workstation must have the laptop plugged into the wire network.

Q3. What if I need software installed or updated?

A. All new or updated software must be installed by Technology and Media Services. Before any software can be installed the vendor user agreement has to be approved by University general council and purchasing. This includes purchased and freeware software titles.

Q4. What if I need software loaded after hours or on the weekend?

A. We can temporary grant administrator rights to those people who need this type of support. All licensing restrictions apply.

Q5. What if some of my software requires administrator rights to run?

A. If we find an application that requires administrator rights to run we will work with the vendor to find a solution that enables the application to run as installed. Most applications can be tweaked to run without the user needing administrator rights. If the software must have administrator rights to run, we will deal with these on a case by case basis.

Q6. What is the policy in other departments on campus, especially the College of Medicine and UIHC?

A. The College of Medicine and UIHC do not allow administrator rights on clinical computers. They do have a firewall at the boarder of their network (which is different than the campus network) which allows them to block specific traffic from entering the hospital network. The main campus network does not have this level of security so we have to treat clinical and non-clinical computers then same. Most academic departments on campus do not allow faculty or staff to have administrator rights on managed computers.

Q7. What is the approved collegiate software and how are nonstandard applications dealt with?

A. Approved collegiate software is what is loaded on all managed computers that we install. This includes but is not limited to Windows 7, 8 and 10, Microsoft software that comes preinstalled with Windows such as Internet Explorer and Windows media player, Microsoft Office, clinic support software such as axium, MiPacs and Dolphin, Adobe Acrobat reader, and Microsoft virus
protection. Any licensed software (Adobe Acrobat Pro, Photoshop, Sidexis (CBCT software) etc.) that the college uses is also on the approved software list.

Resources


http://en.wikipedia.org/wiki/Malware