TEXAS TECH UNIVERSITY
HEALTH SCIENCES CENTER™
INFORMATION SECURITY OFFICE

POSITION PAPER ON: ADMINISTRATIVE PRIVILEGES

Administrator access is a tightly controlled privilege and was removed to reduce the impact of malware outbreaks. This type of access is highly privileged and is only granted under special circumstances. For example, a provider needs administrator rights because a device attached to the system cannot function without it, which in turn affects the level of care to our patients. This is a situation where administrator access will likely be granted.

We must be careful not to violate policy and the principle of least privilege which states that our users are given the minimum privileges necessary to perform the duties assigned. The principle of least privilege is advocated by local (TTUHSC Information Security), state (TAC 202), and federal (HIPAA) policies.

Besides policy, other reasons for not granting administrator rights include:

1. The two most dangerous actions performed on a computer are reading email and using the Internet since these are the primary attack vectors that infect, harm, and otherwise disrupt business operations. This applies for Windows, Macs, and Linux machines equally. All users and systems are susceptible to computer viruses and malware infections. Infections that occur with users who have administrator rights are compounded and can spread rapidly. Controlling administrator rights helps control the spread of a malware outbreak.

2. Given that we are a healthcare, research, and educational institution, such an infection, particularly on the system of an MD, PhD or others who access patient information regularly will lead to a breach of protected health information (PHI) and ultimately to sanctions by HIPAA. It is true that many of our users do not work with PHI, but do not forget that PHI is only one specific example of confidential information. Many other forms of confidential information exist and include FERPA protected student information (for example, grades) and personally identifiable information (PII) such as Social Security Numbers.

For the researchers, your unpublished research and current research activities are also considered confidential information and, in many cases, intellectual property which also has value. And for those users who do not work with confidential information at all, an infection or unauthorized access of your system is an attack vector which can lead to a breach of confidential information. Recall the adage “a chain is only as strong as its weakest link”. Without local administrator rights:

A. An infection cannot spread easily and can remain isolated, thus containing the breach.
B. In the case of unauthorized access, the damage can also be contained.

3. Removing administrator rights is a control that prevents the installation of unauthorized software that can open up security holes in our infrastructure. Further, controlling the installation of software prevents the “my computer is too slow” syndrome since many installed software packages contain agents that constantly run in the background. Controlling administrator rights helps maintain the health of our systems.

The Information Security Office understands that situations exist where administrator access may be beneficial to users. For example, if a user is presenting at a conference from a laptop, there may be fears that a driver or some other piece of software that is needed may prevent the ability to deliver the presentation. In this situation, we are open to providing temporary administrator access to calm your fears.

We are also very willing to work with users where possible and consider other situations on a case by case basis so long as the security posture of our infrastructure is preserved. But the measure by which each case will be considered is the aforementioned principle of least privilege (the minimum required to perform your duties). Unfortunately (and please accept our apologies in advance), convenience does not meet this requirement.

We find in many requests for administrator access, the main reason why it is wanted is to install updates from 3rd parties such as Adobe and occasionally from Microsoft. While these updates can quickly become annoying (we again offer our apologies), this does not meet the principle of least privilege measure.

The daunting task as assigned to the Information Security Office is to protect our institution from the above situations. While on the surface a simple request to grant administrator access seems harmless, but the implications are great.