Computing Security Best Practices

"Why you should not run your computer as an administrator"

Running your computer as a member of the Administrators group makes the system vulnerable to Trojan horses, viruses, and other security risks no matter how careful the user is. The simple act of visiting an Internet site or opening an e-mail attachment can be damaging to the system especially if software such as Flash, Java, and Windows are not up to date. Any Internet site or e-mail attachment may have exploit code that can be downloaded to the system and executed.

If you are logged on as an administrator of a local computer, a Trojan horse could delete your files, corrupt files on network shares, install malicious software & fake antivirus programs, and create a new user account with administrative access capable of leaking personally identifiable information.

Source: Microsoft http://technet.microsoft.com/en-us/library/cc730864.aspx

Approach to Security:
Security of computing infrastructure cannot be assured by one practice or product alone. Security requires layers also known as Defense in Depth. You'll often hear the concept of the layers of an onion used as a metaphor to describe the method used to secure computing services and equipment. Just as safety for an occupant of a vehicle is protected by a bumper, seat belt, and air bag so too must the computing infrastructure be protected from the constant and evolving threats present through many vectors and various forms. The point is that various security mechanisms help to complement each other but they are not dependent on each other. This helps to mitigate single points of failure and weak links.

What TSS is doing:
Some common tasks managed by TSS in regards to computing security include maintaining software updates and deploying them in a timely fashion, providing virus & malware protection on all computers, and filtering of email for malicious content or attachments both from the Internet and messages sent internally, just to name a few. Likewise with our hardware, switches, routers, and other network equipment are updated with newer software when vulnerabilities are reported by the vendor.

The goal of TSS to minimize impact on users and maintain security of Information Systems resources:
TSS implements, to the best of its ability, the concept of least privilege which means giving a user's account only those privileges and rights which are essential to that user's job function. This is because users with administrative privileges on a device can easily circumvent the protections and explicitly tell the virus protection, or the User Account Control (UAC), or whatever protection is in place, that the action to be performed is legitimate thus allowing potentially malicious software to install itself. By implementing the concept of least privilege within our procedures we will be providing better stability, improved security, and easier deployment

In an academic environment the need for exceptions is likely different than that of a corporate environment. Thus, TSS evaluates exceptions on a case-by-case basis.