Short Term Administrative Computer Access Policy

The computer policies of The University of Illinois state that users are not to be logged into computers as administrator unless they are performing administrative tasks. This policy is designed to prevent malicious software from invading a machine and doing damage to that machine and to other computers on the network by altering files that only an administrator has rights to alter. While the IT staff at GSLIS strives to comply with this policy by preventing administrative access to computers throughout the school, we recognize the occasional need for users to be able to install software or adjust settings, often tasks which can only be performed by administrators. To provide users with the access they need when they need it, and still maintain security and comply with campus security policies, the GSLIS Systems Group has developed a technical solution that will allow certain designated users to obtain administrative rights on a machine on a temporary basis. In order to be designated in this way,

1) A user will have to sign a Short Term Administrative Rights and Responsibilities (STARR) agreement, accepting certain responsibilities and recognizing certain risks they will incur in return for those administrative rights. The specifics of the STARR agreement are as follows:

   a) GSLIS will provide an experimental workstation that is initially imaged using standard fully-licensed GSLIS software applications.

   b) The user agrees to install on this workstation only free software or software that is fully and properly licensed to the University of Illinois. If an audit by the GLSIS IT staff finds illegal or dangerous software installed on the workstation, the offending software will be removed by re-imaging the workstation. In that event, any software installed on top of the original image will be removed and will have to be reinstalled by the user.

   c) Since the workstation will be on the network and the user will be logging in under their own login most of the time, they will have access to their own network drive resources (H: drive, for example) and so they should not usually need to save files locally. If any files ***are*** saved to the local machine, the user is responsible for backing up any of those locally-stored files.

   d) The user understands that the experimental workstation, while offering the ability to perform software installs and configurations, also poses some risks that the installed software and any data stored on the machine could be compromised by rogue applications or by virus or worm infections or other hacks. The user understands that in the event of corruption or infection of the workstation, the workstation may be removed from the network and may also be completely re-imaged. Any software that was installed on top of the standard image would then need to be reinstalled by the user.

   e) The user understands that if installing software on the experimental workstation damages software installed in the original image, the damage will be repaired by re-imaging the entire computer. IT staff will not be expected to spend time debugging problems caused by a software install by the user.

   f) The user is to make sure that when installing an application under the administrator login, the application must be configured to be run by normal (non-administrator) users. It is not acceptable to install software that can only be run from the administrator login.

g) The user will not install any services to the outside world on the experimental workstation. Such services include, but are not limited to: Chat Servers (IRC or Messengering Services), Email Servers, Web Servers, Database Servers, Streaming Servers, BitTorrent Servers, or any application that could be used to send large amounts of information to other computers on the internet.

h) The user will be given instructions for obtaining temporary administrative access, and when that access is obtained, that information will be logged. This enables GSLIS to track accountability in the event that the experimental workstation is compromised in some way.

i) Once a user has been given the ability to elevate his or her access to administrative level, this access can be obtained at any time without the user having to consult User Services or the Systems group. Access will be granted for approximately 15 minutes at a time, but can be renewed as many times as it is needed to install software or perform configurations. (This brings us into compliance with the CITES policy that states that users are to be logged in under non-administrative logins *except* when installing or configuring the computer.)

j) The user agrees to abide by the "POLICY ON APPROPRIATE USE OF COMPUTERS AND NETWORK SYSTEMS AT THE UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN" which can be found here:

http://www.fs.uiuc.edu/cam/CAM/viii/viii-1.1.html

2) Once the agreement is signed, users will then have a token added to their LDAP record which will allow them to become a temporary administrator on a designated “experimental” workstation. They will be able to obtain this administrative access at any time, day or night, without having to go through User Services or Systems to get it.

3) The user then connects to the STARR webpage and sets the password for an administrative login on the experimental workstation. This password will expire (and the user will be logged off) in the time shown on the STARR web page for that machine.

4) If the user still needs administrative access after being logged off, they can repeat step 3 above and get a new password.

5) When a user is logged in as an administrator, he or she will not have access to their usual network drive resources, except by manually mapping those drives.

6) User Services will be provided with a DVD that when booted on, will completely re-image the machine. This will make the re-imaging simple and relatively fast, requiring very little work time from User Services personnel or wait time for the user.