

## **Chadron State College Desktop Access Procedure**

### Goals:

1. To ensure that CSC employees are provided access to productive desktop computers required to meet their academic objectives.
2. To create a climate in which all members of the campus community are involved with protecting campus technology resources.
3. To implement access procedures which assure that an appropriate balance exists between the need to protect technology resources and the need to allow users appropriate access to data and applications.
4. To protect technology resources from unauthorized access by viruses, spy-ware and other unauthorized means.
5. To minimize potential support issues caused by open access computers.
6. To allocate support resources to the relevant needs of the campus.
7. To explain the characteristics of the access levels within the CSC environment.

According to Microsoft standards, the Windows 2000 network environment defines three access levels for Windows 2000 and XP operating systems; Normal User, Power User, and Administrative User. According to Apple standards, two access levels are defined for the Mac OS X operating system; Normal User and Administrative User.

By default, computers running Windows XP, 2000, and OSX are configured with the Normal User access level. The Normal User access level provides a solution in which users can run applications with the systems secured against the three most common forms of attack (spy/malware, viruses, and software vulnerabilities). Because of the high level of system protection, the Normal User access level minimizes interruptions for the user, stabilizes the network environment, and reduces the support demand on Information Technology personnel.

To advance to a Power User or Administrative User, an individual shall

- Read the Access Level Description Table and Detailed Access Level Descriptions
- Complete the Request for Elevated Access Level Form
- Submit the form to the Director of Information Technology

Department of Information Technology will

- Establish the elevated access level for the user on the requested computers
- Maintain a log of users with an advanced access level and systems on which access is granted
- Provide timely re-imaging services in response to a service request and document such service

## Access Level Description Table

	<u>Normal User</u>	<u>Power User</u>	<u>Admin User</u>
<u>Level of:</u>			
System Protection	High	Limited	User Controlled
User Responsibility	Low	High	High
Computer Support	Low	Moderate	High
Service Priority	High	Moderate	Low
<u>Risk of:</u>			
Virus Infection	Low	High	High
Spyware/Malware Infection	Low	High	High
Software Vulnerability attack	Low	Medium	High
<u>Responsibility for:</u>			
Operating System Updates	CS	CS	User*
Troubleshooting	CS	User*	User*
Virus Updates/Cleanup	CS/CS	User*	User*
Spyware Updates/Cleanup	n/a	User*	User*
Application Software Installation	CS	User*	User*
Application Software Execution	User	User*	User*
Licensing Compliance	CS	User*	User*
Copyright Law Adherence	User	User	User
Data Backup	User**	User**	User**
<u>Modification of:</u>			
Core Registry	Denied	Partial	Allowed
System Folder	Denied	Partial	Allowed
System Files	Denied	Partial	Allowed
Network Settings	Denied	Partial	Allowed
Program Files Folder	Denied	Allowed	Allowed
Basic User Settings (screen saver, desktop appearance)	Allowed	Allowed	Allowed

\*Users granted the Power User and Administrative User access levels must following licensing policies and compliance. These individuals should have the computer expertise to support and troubleshoot their own software. Should they have trouble with data or application or operating system software that they are unable to resolve, they are responsible for backing up their data and the Department of Information Technology will re-image their system to the standard base image. The end user is responsible for restoration of their data and installation of software beyond the base image.

\*\*The Department of Information Technology strongly recommends that all users, regardless of access level, save all data (including programs they install on their own) in the Documents folder at the root of the hard drive (C:\Documents). Users are responsible for the routine backup of the data on their systems. Backup of that data is greatly simplified by using the single Documents folder location. Backup options may include: Z-drive, zip disks, CD-Rs, and USB jump drives. Data on the Z-drive is backed up nightly by Information Technology personnel.

## Detailed Access Level Descriptions

### 1) Normal User:

Highest Level of Protection, Low User Responsibility, Minimal Computer Support Required

- Benefits:
  1. Due to automated updating controlled by the Department of Information Technology, the user does not need to perform Windows updates, virus scanner updates, or spyware sweeps.
  2. Due to the restricted access to system files, systems cannot be infected by most network spread spyware/malware and viruses. Does not prevent infection due to a user opening an infected e-mail attachment, for example.
  3. User can run most software once it has been installed by Information Technology personnel.
  4. User can modify basic user settings (screensaver, desktop appearance, etc.).
  5. User can modify files within the C:\Documents and Z:\ directories.
- Restrictions:
  1. User cannot install any software that modifies the core registry or system folders or program files folders.
  2. User cannot modify any systems files or network settings.
- Concerns:
  1. The three most common risk factors are minimized at this level, however there is still a risk of computers being damaged by virus infected files opened prior to scanning.

### 2) Power User (Not available on the Macintosh OS)

Limited Protection, High User Responsibility, Moderate Level of Computer Support Required

- Benefits:
  1. Due to automated updating provided by the Department of Information Technology, the user does not need to perform Windows updates.
  2. Due to the ability to modify Program Files folders and most system files and areas of the registry, the user can install some software.
  3. User can modify basic user settings (screensaver, desktop appearance, etc.).
  4. User can modify files within the C:\Document and Z:\ directories.
- Restrictions:
  1. Depending upon the type of spyware, a user may not be able to remove spyware even though it was installed with their access level
  2. User cannot modify all system files and settings or network settings affecting the ability to install software and customize the computer.
- Concerns:
  1. System can be infected by most network spread spyware/malware and viruses so the end user is responsible for regular scans and updating of the detection/removal software.
  2. User has the ability to disable the virus scanner so they are responsible for making sure it is active and updated.
  3. Because the user has the ability to load software, they may unknowingly violate CSC licensing agreements.
  4. User may install software that places a burden on the network and/or infects other campus computers and mission critical servers.

### 3) Administrator

Unprotected, High Risk, High User Responsibility, High Level of Computer Support Required

- Benefits:
  1. User has full access to the computer to install software and customize system.
- Restrictions:
  1. Nothing restricts the user.
- Concerns:
  1. Although the user does not need to perform Windows or anti-virus updates, they are responsible for making sure the settings do not change and verifying that the updates are occurring. Failing to do so risks system and network infection.
  2. System can be infected by all spyware/malware and viruses so the end user is responsible for regular scans and updating of the detection/removal software.
  3. The Department of Information Technology has to monitor network traffic to determine if the system becomes infected and if an infection occurs, determine the extent of the infection.
  4. Because the user has the ability to load software, they may unknowingly violate CSC licensing agreements.
  5. User may load software that places a burden on the network or attacks computers on campus including the mission critical services.
  6. User may modify network settings that could disrupt or disable the campus network.
  7. Users are expected to obtain the skills necessary to resolve system problems and expect re-imaging service from the Department of Information Technology.

Effective: [July 27, 2005](#)

Revised: [June 2010](#)

Publicized:

[MyCSC Forms Repository: August, 2007](#)

**Chadron State College**  
**Department of Information Technology**  
Request for Elevated Access Level

Name:

Department:

CSC Tag# of Computer(s):

- I have read the Access Level Description Table and Detailed Access Level Descriptions.
- I accept the below listed responsibilities associated with the elevated access level as stated in the Access Level Description Table and certify that I have the knowledge and skills necessary to fulfill the responsibilities:

- Data Backup
  - Operating System Updates (Windows/MacOS)
  - Virus Updates/Cleanup
  - Spyware Updates/Cleanup
  - Troubleshooting
  - Application Software Installation
  - Application Software Execution
  - Licensing Compliance
  - Copyright Law Adherence

- I understand that in the event the computer to which I have elevated access requires service, the computer will be re-imaged by Information Technology personnel. This will result in the deletion of all files and data and the installation of the base image. It will require that I reinstall my software from software distribution media that I possess and my data from backup media that I possess. **It is imperative that data is backed up on a regular basis.**
- I will maintain regular computer connectivity to the campus network.
- I will keep automated protection mechanisms including operating system updates and anti-virus updates enabled.
- I will keep the computer and network secure. I will not create additional computer accounts on the computer or provide my username/password to others.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

IT Signature: \_\_\_\_\_

Date: \_\_\_\_\_

To: Dr. Janie Park  
Dr. Lois Veath  
Dr. Randy Rhine  
Cc: Mr. Dale Grant  
Fm: Ann Burk  
Dt.: April 23, 2007  
Re: Desktop Access Procedure

Following a review of the desktop access procedure with Keith Crofutt and Starr Giorgi, I have created a form to be completed by individuals requesting to install software on the computers to which they are assigned. Dale has reviewed the form and provided comment.

Please take a critical look at it and provide me with your suggestions.

Also included are the supporting documents that will be provided on the web site.

As always, I would be happy to answer questions or discuss the procedure further.