Chadron State College
Desktop Access Procedure

Goals:

1. To ensure that CSC employees are provided access to productive computer 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 and in compliance with the Information Security Policy.
4. To protect technology resources from unauthorized access by malware 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 network environment defines two access levels for Windows operating systems; Normal User and Administrator. According to Apple standards, two access levels are defined for the Mac OS operating system; Normal User and Administrator.

By default, computers running Windows and Mac OS 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 most common forms of attack (malware 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 Administrator access on a computer, an individual shall

- Read the Access Level Description Table and Detailed Access Level Descriptions
- Indicate an understanding of the responsibilities associated with Administrator access to a computer.
- Complete the Request for Administrator Access Level Form
- Submit the form to the CIO/Information Security Program Coordinator for review and approval by the IT Leads.

Information Technology will, upon approval

- Verify that the individual does not have access to data classified as protected or restricted as per the Information Security Policy. Having such access denies Administrator access.
- Establish the Administrator 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

	Normal Access	Administrator Access
Level of:		
User Responsibility	Moderate	High
Technical Support	Low	High
Risk of:		
Malware Infection	Low	High
Software Vulnerability attack	Low	High
Responsibility for:		
Operating System Updates	IT	User*
Troubleshooting	IT	User*
Malware Updates/Cleanup	IT	User*
Application Software Installation	IT	User*
Licensing Compliance	IT	User*
Copyright Law Adherence	User	User
Data Backup	User	User

*Users granted Administrator access level to a computer 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 Information Technology will re-image the system with the standard base image. The end user is responsible for restoration of their data and installation of software beyond the base image.

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: Office 365 One Drive, CD-R and USB jump drives.

Automated and regular updates are installed using KACE Management Appliance. This includes and is limited to the Windows & Mac operating systems and Symantec Endpoint Protection.

Users with access to applications containing data classified as protected or restricted as per the Information Security Policy will not be granted Administrator access unless the application requires Administrator access level for application functionality.

Detailed Access Level Descriptions

1) Normal:

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

- Benefits:
    1. Due to automated updating controlled by Information Technology, the user does not need to perform Windows updates, virus scanner updates, or malware sweeps.
    2. Due to the restricted access to system files, systems cannot be infected by most network spread malware. 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.
    4. User can modify basic user settings (screensaver, desktop appearance, etc.).
    5. User can modify files within the C:\Documents and mapped 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 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 or infected devices connected directly to the computer (USB, etc.).

2) Administrator:

Unprotected, High Risk, High User Responsibility, High Level of Technical 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 malware so the end user is responsible for regular scans and updating of the detection/removal software.
    3. 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 and other licensing agreements.
    5. User may load software that places a burden on the network or attacks computers on campus including critical services.
    6. User may modify network settings that could disrupt or disable the campus network.
    7. Users are expected to possess the skills necessary to resolve system problems.
    8. Users are to understand that IT will resolve issues by re-imaging the computer.

Effective: July 27, 2005 as approved by Executive Staff
Revised: July 2007
Revised: July 2017

Publicized:
CSC Web Page-August, 2005
Faculty Handbook-August, 2005
MyCSC Forms Repository: August, 2007

As per the 20017-2019 SCEA Agreement:
In compliance with college procedures which require prior disclosure, faculty members , may load or have loaded licensed, academic-specific software on their office computers. Approval to load software shall be made in a timely manner and shall not be unreasonable denied. A denial to load software must specify in writing the reasons for such denial.

Chadron State College
Department of Information Technology
Request for Administrator Access

Name:	**CSC Email Address:**
Department:	**CSC Tag# of Computer(s):**
Purpose for Administrator Access:	

- I have read the Desktop Access Procedure Document, specifically the Access Level Description Table and the Detailed Access Level Descriptions.

- I accept the responsibilities associated with Administrator access as stated in the Access Level Description Table and I have the knowledge and skills necessary to fulfill the responsibilities:
  - Technical Support of the Computer
  - Operating System Updates (Windows/Mac)
  - Troubleshooting
  - Malware Updates/Cleanup
  - Application Software Installation
  - Application Software Execution
  - Licensing Compliance
  - Copyright Law Adherence
  - Data Backup

- I understand that in the event the computer to which I have Administrator access requires service by Information Technology, the computer will be re-imaged by Information Technology. This will result in the deletion of all files and data and the installation of the base image. It will be my responsibility to reinstall software from licensed software distribution media that I possess and restore data from backup media that I possess.

- I understand that 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 malware 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.

- I understand that in the event my account is granted update access to an application containing Protected or Restricted data as per the Information Security Policy, Administrator access will be removed.

Requestor Signature:_____Date: _____

Department of Information Technology Use

Information Security Validation (check all that apply):
- ☐ *CSC Tag# is assigned to Requestor in the asset database*
- ☐ *Requestor does not have access to Protected or Restricted data as per the IS Policy*
- ☐ *Request reviewed by IT Team Leads and CIO/IS Program Coordinator*
- ☐ *Request approved and moved to IT Specialist for activation of Administrator access*
- ☐ *Request denial reason attached and returned to Requestor via e-mail*

CIO/IS Program Coordinator Signature/Date: _____

Activation (check all completed):
- ☐ *Administrator access activated*
- ☐ *Requestor notified via e-mail*
- ☐ *Completed form submitted to IT Support for upload to SharePoint*

IT Specialist/Analyst Signature/Date: _____ Date: _____