
INFORMATION TECHNOLOGY SERVICES POLICY

Name of Policy **USD Network Access Policy**

1. Purpose

The purpose of this policy is to clearly outline appropriate use of the USD network resources.

2. Scope

The scope of this policy includes all individuals connecting to the USD network; including, but not limited to Faculty, Staff, Students and Affiliates.

3. Definitions

4. Policy Statement

One of The University of South Dakota's primary goals is to keep our local network and Internet connections functioning and serving the academic needs of our students, faculty and staff.

4.1 Authorized Equipment

All equipment must be purchased by USD or an Affiliate Organization who has been granted a waiver by the Vice President of Information Technology. Equipment must meet minimum requirements.

4.1.1 University owned Computers

4.1.2 Network printers and multi-function copiers

4.1.3 Personal computers connected via the Clean Access Agent. Reference the Personal Computer support policy for additional information
<http://www.usd.edu/its/docs/Personal-Computer-Support-Policy.pdf>

4.1.3.1 Personal computers will not be added to the USD domain. Faculty and staff should use university provided equipment when performing their official duties.

4.1.4 Servers

4.1.4.1 Server Hardware must be approved by ITS

4.1.4.2 The USD Domain Administrator group must have full access rights to the server

4.1.4.3 All approved servers must be located in an ITS designated Machine room

4.1.4.4 Department servers must have prior written approval from the Vice President of Information Technology

4.2 Unauthorized Equipment

4.2.1 Servers

4.2.2 Local resource sharing including but not limited to printers and data storage

4.2.3 Equipment that allows more than one computer or device to connect through a single connection (port) including but not limited to the following:

- 4.2.3.1 Switches
- 4.2.3.2 Hubs
- 4.2.3.3 Routers
- 4.2.3.4 Wireless access points

4.3 Network Protection

- 4.3.1 All computers must have USD approved anti-virus software installed
- 4.3.2 Each computer connected to the network will be scanned for viruses weekly
- 4.3.3 Each computer will receive all necessary updates to anti-virus and operating system when they are released
- 4.3.4 If you suspect your computer has been infected with a virus, contact the Help Desk immediately
- 4.3.5 Should you receive a warning about viruses from anyone other than the ITS Help Desk, DO NOT forward them to anyone except the Help Desk. Information Technology Services will evaluate the veracity of the warning and take appropriate action. Many of these warnings are hoaxes
- 4.3.6 DO NOT ever share your USD password with anyone. Any requests you receive for your password should be reported to the Help Desk immediately
- 4.3.7 Any hacking of the network, denial of services (DoS) attacks, spamming or virus/worm dissemination or other malicious attacks will not be tolerated
- 4.3.8 Access to computer resources from off campus must be done using only methods approved by the VP of Information Technology. Remote access software such as PCAnywhere and VNC are prohibited. Users may instead use the remote access services provided by the University – http://www.usd.edu/its/techsupport/offcamp_access.cfm.
- 4.3.9 Network infrastructure devices connecting to the network are prohibited. Exceptions must be approved by the VP of Information Technology. This includes wireless access points, hubs, switches, routers, etc. Personally owned devices are not authorized and will not be granted approval.

4.4 Faculty/Staff Network Storage

- 4.4.1 No personal photos, music or video files (mp3, m4p, wav, etc.) should be stored on the university network. Materials used for conducting university business are the exception.
- 4.4.2 Your "My Documents" folder will be redirected to your University network file space to ensure appropriate back-ups are complete for your data used for conducting university business
- 4.4.3 Document sharing should not be done through computers, and personal network User folders. Contact the Help Desk to request the necessary sharing folders.

- 4.4.4 If you have large volume storage needs contact the Help Desk for permission prior to storing data on the network.
- 4.4.5 Contact the ITS Help Desk if a vendor requires access to any USD network resources.

4.5 Reporting a password compromise

- 4.5.1 Suspected compromises of passwords must be reported immediately to the ITS Help Desk at 677-6463 or toll free at 877-225-0027.
- 4.5.2 The password in question should be changed immediately at <https://www.usd.edu/accounts/reset>.

4.6 Password Auditing

- 4.6.1 ITS may require a more restrictive policy, such as stronger passwords, in some circumstances
- 4.6.2 ITS or its delegates may perform password assessments on a periodic or random basis. If a password is guessed or cracked during one of these assessments, the customer will be promptly notified and required to change their password. Again, the current password will NOT be sent or requested by e-mail from ITS

5. Consequences

Any violation of the above policy may result in a loss of network connectivity. In addition, the incident may be reported to the appropriate authorities.

6. Revision History

Date	Change	Made By