UNIVERSITY OF SOUTH DAKOTA

Policy Number:	5.011
Originating Office:	Information Technology Services
Responsible Executive:	Vice President for Administration and Technology
Date Issued:	10/11/2011
Date Last Revised:	08/05/2015

Network Access

Policy Contents

I. REASON FOR THIS POLICY

One of the primary goals of Information Technology Services (ITS) at USD is to keep our local network and Internet connections functioning and serving the academic needs of our students, faculty and staff. Certain network devices, if deployed incorrectly or if malfunctioning, can disrupt connectivity for the entire University community.

The purpose of this policy is to clearly outline appropriate use of, and connections to, USD network, data storage and computing resources. This policy applies to all individuals connecting to the USD network; including but not limited to faculty, staff, students and affiliates.

Policy last reviewed 8/5/15 by the CIO Management Team

II. STATEMENT OF POLICY

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

University-owned Equipment

1. Any networking device or server owned by individuals or departments outside of ITS and not having written approval from the Vice President of Administration and Technology is considered unauthorized and must not be connected to the University network.
2. All networking devices and servers must be procured and maintained by ITS. All computing equipment purchases must be approved by ITS. Affiliate Organizations may

be granted a waiver by the Vice President of Administration and Technology for the purchase of designated computing equipment.

3. All computing equipment, networking devices, and servers must meet minimum requirements published by either USD or the Board of Regents (BOR).
4. Authorized servers and networking devices must be located in machine rooms designated by ITS. ITS will designate individuals who must be given administrative privileges on all authorized servers and networking devices.
5. Whenever feasible, computing equipment will be configured to connect to network file storage. Personal files (including multimedia files such as images, audio, or video) must not be stored on University-owned servers. Only files that are necessary for conducting University business are permissible. Files which constitute a significant amount of storage space must be approved by ITS.
6. Authorized servers will be periodically backed up. Stored backup data will be maintained in a fireproof safe.
7. Computing equipment must have USD-approved anti-virus software and be scanned for viruses weekly.
8. Computing equipment will be configured to receive all necessary updates to its anti-virus software and operating system periodically.

Personally-owned Equipment

1. Personally-owned computing equipment may be connected to the network at USD campuses only if the equipment meets the standards enforced by USD's network access control system.
2. Personally-owned computing equipment must not be used as a server or networking device.
3. Personally-owned computing equipment will not be added to the USD domain.

III. DEFINITIONS

Computing Equipment: Personal computing devices that utilize the wired or wireless network to transfer data; including, but not limited to, desktop computers, laptops, tablets, smart phones, and game consoles.

Networking Devices: Any device whose purpose is to transfer data to and from computing equipment; including, but not limited to, switches, routers, firewalls, wireless-access points, and Apple TV's.

Server: Any computer or device whose purpose is to provide a network service or storage to computing equipment; including, but not limited to, network-attached storage (NAS) devices, networked printers and multifunction copiers, and any computer running a network service.

Network Service: A software application which provides access to a resource via network requests from computing equipment; including, but not limited to, file and printer sharing, web servers, and Dynamic Host Configuration Protocol (DHCP) servers.

Network Access Control System: A system of hardware and software which enforces network policies for connected clients in an effort to secure the network. Policies include, but are not limited to, antivirus software, system updates, and system configuration.

IV. PROCEDURES

Procuring University-owned Computing Equipment

- Go to https://portal.usd.edu/technology/support/faculty-staff/hardware-purchasing.cfm for help with purchasing standard computing equipment which can be supported by USD ITS.
- Go to https://portal.usd.edu/technology/support/standard-hardware-support.cfm for the minimum requirements of hardware which can be supported by USD ITS.
- Contact the Help Desk for projects which require more specialized equipment such as servers or networking devices.

Granting Administrative Privileges to USD ITS

- On an authorized Windows system, add the Domain Administrators group to the local administrators group.
- On an authorized Linux or Unix system, provide super user privileges/role to designated ITS employee accounts.

Computer and Network Protection

- Go to http://www.usd.edu/technology/getting-connected-on-campus for help with installing antivirus software or configuring system updates and patches on personally-owned computing equipment.
- If you suspect your computer has been infected with a virus, contact the Help Desk immediately.
- 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.

Faculty/Staff Data Storage and Sharing

- For document sharing, contact the Help Desk to request the necessary sharing folders.
- If you have large volume storage needs contact the Help Desk for permission prior to storing data on the network.
- Contact the Help Desk if a vendor requires access to any USD network resources.

V. RELATED DOCUMENTS, FORMS AND TOOLS

USD Personal Computer Support Policy 5.013

USD Remote Access Policy 5.012

USD User Passwords Policy 5.008

Board of Regents Acceptable Use of Information Systems Policy 7:1 - https://www.sdbor.edu/policy/documents/7-1.pdf