Network Connection Standard

Document Number:	ISP-018	**Version:**	1.1
Document Owner:	Director of Information Security Deputy Director of Network Engineering	**Effective Date:**	06/22/2020
Responsible Office:	Office of Information Technology	**Last Update:**	03/29/2021

TABLE OF CONTENTS

PURPOSE [TOP]

The purpose of this standard is to establish the ownership, administration, permissible actions, and acceptable use of the campus network to connect to University information systems and resources, as well as to off-campus resources. All connections, whether local or remote, to information systems must follow enterprise standards and best practices, and be centrally administrated; in limited instances, exceptions may apply.

This standard is in place to safeguard the information system user, the information system, and the University; comply with legal and contractual requirements; and protect the University against damaging legal and financial consequences. Inappropriate use and configuration expose the University to risks including viruses, compromise of network systems and services, financial considerations, and legal issues. This standard requires that the users of information assets to comply with University policies, standards, and procedures to protect the University.

SCOPE [TOP]

The scope of this standard includes all Southern Illinois University Carbondale (SIUC)-affiliated personnel (see Roles and Responsibilities) who, through the course of that affiliation, require access to network resources and University software and services.

Additionally, this standard applies to all systems that contain, process, or transmit electronic information related to SIUC. In this context, "systems" include servers, workstations, devices, hardware, network including the internet, processes, and electronic data. This standard applies to all activity originating from, directed to, existing on, and/or traversing the system.

It is the responsibility of the University Chief Information Officer (CIO), or designee, to determine whether a particular use of network resources conforms to University, policy, standards, and guidelines.

STANDARD [TOP]

All members of the University community have a responsibility to use systems and network resources in an approved, ethical, and lawful manner to avoid loss or damage to University operations, image, or financial interests and to comply with all official acceptable use policies, standards, and procedures.

Pursuant to this responsibility, users of systems and network resources related to SIUC shall abide by the standards in this document, in letter and spirit, in order to establish the acceptable use of the campus network and connected systems for the purposes of protecting the University and to enable compliance with laws, regulations, policies, requirements, standards, and other appropriate criteria.

The University and the Office of Information Technology (OIT), reserves the right to modify, add, or delete portions of this standard without notice; to protect students, staff, and the University from potential unknown or future security threats.

SIUC network is comprised of various devices, protocols and technologies that create a system of connectivity for the sole use of the education, research, administration, and public service pursuits of the university. Controls are implemented to safeguard the operation and stability of this essential service including, but not limited to:

- Connection of devices
- Network Traffic
- Security
- Scanning
- Remote Access
- Auditing and monitoring
- And Use

All items that are governed under this standard remain the sole domain of OIT. Specific requirements for various technology and devices are included below. This is not to be considered an exhaustive list and will be updated and augmented periodically. Non-OIT use of the SIUC network is for end-user devices only, such as desktops, laptops, workstations, mobile devices, etc. Other uses are subject to review and approval by the OIT.

A. Network Connectivity

1. As with any system or network resource at SIUC, the Acceptable Use Standard applies.
2. IP Addresses
    a. Under no circumstance may any connected device be configured with IP addresses that have not been assigned by the OIT. Using an unregistered IP address, or IP address assigned to another, may deprive other users of a network service(s) and/or make it difficult to diagnose problems on the campus network. Dynamically assigned IP addresses (DHCP) are “registered” for the period of the dynamic lease to a given system.
3. MAC Addresses
    a. Using a different Ethernet hardware address (MAC) other than is assigned by the manufacturer will result in the device being removed/blocked from the campus network. In the event a MAC address changes due to a hardware change, it is the responsibility of the system owner to inform the OIT in order to ensure that the information and registration of the system is accurate and up to date.
    b. Use of an unassigned/inaccurate IP address and/or MAC address different than the one registered with the OIT is grounds for removal from the network and/or suspension or loss of campus network privileges.
4. Remote Connections

a. Remote connections to campus that are not allowed through the SIU Internet/edge firewall, must utilize the OIT-provided VPN or VDI service and must be in accordance with the campus Remote Network Connection Standard. All other remote connectivity is prohibited. Please refer to the Remote Network Connection Standard for more details.

5. Restricted Devices
    a. DHCP Servers
        i. Systems on the campus network are not permitted to be configured as DHCP servers. DHCP allows systems to obtain the correct IP address during the boot process. User-owned DHCP servers might override the distribution of IP addresses by the official campus DHCP servers, causing the client system to obtain an incorrect address, denying it access to the network. Any system found to be running a DHCP server will be immediately removed from the network.
    b. Routers and Wireless Access Points
        i. No routers or wireless access points will be allowed to be attached to any portion of the campus network without specific written approval from the OIT. Any devices which provide routing service or wireless access, will be immediately disconnected from the campus network until such capabilities have been disabled. Repeat offenders are subject to suspension or loss of their network connection privileges.
        ii. Routers are generally used to connect multiple network segments together and should not be necessary for individual users on campus. If misconfigured, routers can cause severe problems for all users on a network segment. Even if properly configured, routers can cause significant difficulties with the maintenance and support of network segments maintained by OIT.
    c. External Network Connections
        i. Any network-attached device that connects the SIUC data network to any external network is strictly prohibited, unless administered by OIT. This includes devices such as, but not limited to; T1s, DSL modems, gateways, dedicated connects, etc.
    d. Other Restricted Devices and Activities

i. Any other network-attached device that has the capability of impacting data of another network user is strictly prohibited. Such items include, but are not limited to: DNS servers, Email servers, NAT/PAT router/routing, firewalls, web proxy, SSL decryption, intrusion detection/prevention systems (IDS/IPS), packet capture attempts, unauthorized network scans, network access controls (NAC), unauthorized switches, etc.

B. Network Traffic

Network traffic is considered private. Thus, any "packet sniffing," or other deliberate attempts to read network information which is not intended for your use is strictly prohibited and will be grounds for loss of network privileges for a period determined by the CIO or designee and referred to administration for disciplinary action. In some cases, the loss of privileges may be permanent. Note that it is permissible for the OIT system owners/administrators to run a packet sniffer explicitly configured in promiscuous mode to troubleshoot connectivity issues.

It may not remain feasible to provide unlimited bandwidth for systems which are not strictly serving the University's missions. Because of this possibility, the OIT reserves the right to control the network traffic generated by any system, or where necessary, to remove such systems or services from the campus network.

If a system is unintentionally misconfigured and subsequently causes a problem on the campus network, the machine will be disconnected from the campus network.

C. Security

Users are responsible for the security and integrity of their systems. In cases where a device or system is compromised, or suspected to be, the system will be shut down or be removed from the campus network immediately to localize any potential damage and to stop the attack from spreading. Please see the following for more information:

Incident Response Standard

Incident Response Procedure

In such cases, if the system administrator cannot be contacted in a reasonable time, OIT reserves the right to disable the network connection. Once the system administrator is

made aware of the situation and agrees to take reasonable steps to ensure that the machine is not compromised or has been cleaned/reinstalled, network privileges may be restored.

D. Network Scans

OIT will periodically conduct scans of the network for a variety of management activities. Results of such scanning may help OIT to discover misconfigured systems and may in some cases discover activity which violates laws, university policies, or OIT standards or guidelines. In such cases, appropriate action will be taken. All other network scanning is strictly prohibited.

E. Commercial Use

Under no circumstances will any individual be permitted to use their network connection or computing privileges for commercial purposes. Any commercial use of campus facilities is explicitly prohibited by the University and is grounds for removal of campus network privileges.

Any system that provides services for a commercial operation (e.g. a website selling commercial products), provides services of a commercial nature (e.g. provides web services for a fee) is explicitly prohibited from the campus network.

In limited instances, exceptions may apply.

F. Remote Access

External (defined as off-campus) access to information systems is governed by system classification and authorized based on user roles and responsibilities. Remote Desktop (RDP) is authorized utilizing standard RDP methods (e.g. Microsoft RDP, Apple Remote Desktop, Linux VNC/SSH). To maintain system integrity and security, all external RDP traffic must pass via the campus VPN; RDP ports are disallowed at the campus network boundary. Attempts to circumvent this security measure are in violation of this standard.

Any software or application that allows remote connections to bypass the VPN and/or Edge Firewall is specifically prohibited. Additionally, the OIT offers VDI as an alternate method of remote access.

Please refer to the Remote Network Connection Standard for more details.

G. Audit and Accountability

Any system connected to the campus network is required to create, protect, and retain system audit records to:

- Enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or in appropriate information system activity.
- Ensure the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Any multi-user system (i.e. database server, web server, application server, etc.) connected to the campus network is required to maintain the same audit records and forward those logs to the central OIT log server.

H. Exceptions and Exclusions

Any exception or exclusion request must be submitted in writing, reviewed, and approved by the CIO or designate.

ROLES AND RESPONSIBILITIES

[TOP]

All SIU personnel including, but not necessarily limited to, students, faculty, staff, retirees, outsourced contractual workers, guests, alumni, volunteers, temporary extra help, student workers, graduate assistants, undergraduate assistants and vendors are required to abide with the requirements and standards established within this standard.

DEFINITIONS

[TOP]

IP Address – Internet Protocol Address. A unique identifier either statically or dynamically assigned to network connected devices, and which allows for communications on a local network and the Internet.

MAC Address – Media Access Control Address. The unique identifier that is manufacturer assigned to network interface hardware, or otherwise known as ethernet hardware.

Network/Data Network – The campus voice and data network.

Packet Sniffing – Capturing data from a network by a recipient for whom that data is not intended. Can be a troubleshooting tool or used for nefarious purposes.

RDP – Remote Desktop Protocol. Enables the ability to remotely access a computer as though the user were local and not remote.

VDI – Virtual Desktop Interface. The hosting of desktop environments on a central server. It is a form of desktop virtualization, as the specific desktop images run within virtual machines (VMs) and are delivered to end clients over a network.

VPN – Virtual Private Network. A system that allows for secure communications to a network from a remote site.

SSH – Secure Shell. Software that allows secure, remote management of computing resources.

COMPLIANCE [TOP]

Violations of this standard may result in suspension or loss of the violator's use privileges, with respect to Institutional Data and University-owned Information Systems. Additional administrative sanctions may apply up to and including termination of employment or contractor status with the University. Civil, criminal, and equitable remedies may apply.

REFERENCES [TOP]

ISP-009 Incident Response Standard

ISP-010 Incident Response Procedure

ISP-013 Acceptable Use Standard

ISP-019 Remote Network Connection Standard

AUTHORITY [TOP]

Southern Illinois University Board of Trustees Policy, SIU System Information Security Plan.
Southern Illinois University Carbondale Information Security Program (ISP).

REVISION HISTORY

[TOP]

Version	Description	Revision Date	Author
1.0	Standard was approved by CIO	06/22/2020	Director of Information Security Deputy Director of Network Engineering Director of Technology Services
1.0	Hyperlink corrected	06/23/2020	Associate Director, PMO
1.1	Reviewed and updated with minor changes for readability and clarification	03/29/2021	Director of Information Security Deputy Director of Network Engineering