PROCEDURE TITLE:	CONDITIONS FOR USE OF UNIVERSITY COMPUTING RESOURCES
PROCEDURE NO.:	5.30:1
RELATED POLICY:	5.30REV
PAGE NO.:	1 OF 6
RESPONSIBLE ADMINISTRATOR:	DIRECTOR OF IT OPERATIONS
EFFECTIVE DATE:	06/21/2024
NEXT REVIEW DATE:	06/2027
APPROVED BY:	PRESIDENT

These *Conditions for Use* provide comprehensive details that serve as standard operating procedures for two major information technology areas: Section 1: Network Access; and Section 2: Application Computing.

The information describes the conditions for users to gain access and authorized use of Shawnee State University's information technology systems, network, and applications. Implementation of and adherence to security guidelines and best practices to protect confidential information and Institutional Data are the responsibility of all University users. All users are responsible for understanding and complying with these *Conditions for Use*, in addition to the Information Security Program procedures.

1.0 NETWORK ACCESS

As part of the physical, administrative and academic infrastructure, Shawnee State acquires, develops and maintains computers, computer systems and networks. These computing resources are intended for appropriate university related business performed by employees or designated delegates.

The use of university computing resources, similar to the use of any other University-provided resource, is subject to the requirements of legal, regulatory, and ethical behavior within the University community.

1.1 Policy 5.30Rev. permits access to computing resources and is applicable to current and former students, faculty and staff, agents, contractors, volunteers, vendors and sponsored guests of the academic and administrative units, and affiliated entities, and to all users of the University's computing and network resources, regardless of location or device.

1.2 Access to computer programs and network resources requires a written request which must come from the department of Human Resources to the IT Service Desk. Access to information which is private or confidential will be restricted.

1.3 Employees who leave the employment of the institution shall have their account access disabled and all of their files will be deleted 30 days later after documents of a departmental nature are identified and appropriately dispositioned. Those employees who have been terminated or have received notification of termination will promptly be restricted from access to the system upon notification to the IT department from Human

Resources, a Senior Executive, or the department supervisor. In this procedure Senior Executive means the President, Vice President for Academic and Student Affairs/Provost, Chief Financial Officer, Chief Operating Officer, Chief Enrollment Officer, Chief Advancement Officer, Chief of Staff, and any other Vice President or Chief level positions created after the enactment of this procedure. Faculty, per the SEA collective bargaining unit, who retire with at least 10 years of service may request to keep the SSU email address they currently have. This request must be made during the exit interview with HR. The faculty account will be disabled on the last day of employment, deleted 30 days later and the new retiree email account will be created at that time with the same user name.

1.4 Access to on-campus computers and networks requires a means to authenticate a user's identity, usually with a username and password. The user, or account owner, is responsible for all actions originating from an assigned account. Passwords to protected accounts may not be shared or used by anyone other than the assigned user.

1.5 Users given access to university computing resources shall be advised of their access. Users may not go beyond or attempt to go beyond their assigned access without authorization.

1.6 The installation/execution of games and/or recreational programs and devices on Shawnee State systems excluding those required for academic coursework or the use of E-Sports team in designated labs and classrooms intended for gaming, is prohibited.

1.7 Use of University computer systems, resources, networks and/or services for unauthorized commercial activities, including use of Internet facilities for any commercial activities, is prohibited.

1.8 Access to all University networks via an approved personal computer or device is conditioned on adherence to meeting established prerequisites and specific rules listed below. Since the wireless network is an “always on connection” similar to commercial broadband, the University has a responsibility to both the wireless network users and the greater Internet community.

1.8.1 Users are ultimately responsible for securing their personal computer systems. The University’s network is continuously monitored for malicious, unauthorized and inappropriate activity. If issues are detected on a personal computer system, the owner of that computer will be notified of the action necessary to resolve the problem.

1.8.2 If the action results in the disconnection of that user from the network, they will be advised of the required steps to be reconnected to the Network. Upon satisfaction that all steps for reconnection have been met, in order for the user to reconnect a device to the network after a virus or other malicious software has been removed, an appointment with an ITS Technician may be necessary to verify the hard drive in question has been cleaned.

1.9 Specific Rules: The following specific rules are not optional and apply to all individuals connecting to the wireless network:

1.9.1 No servers of any kind will be allowed on the network. Specific examples of servers are: Web servers (Apache, Windows Personal Web Server, etc.), FTP servers (Serv-U, WS-FTPD, etc.), File sharing servers, and Gaming servers.

1.9.2 Personal devices are not allowed to connect to SSU's wired networks. Furthermore, devices such as wireless access points, thin-clients, hubs, switches, routers, print servers, and network appliances are strictly prohibited.

1.9.3 Network port scans will not be allowed. Port scans may be performed by ITS to maintain the network. However, no individual is to perform a port scan of any host inside or outside of the Network. This will be considered a network attack.

1.9.4 Network attacks of any kind will not be tolerated. Network attacks are serious concerns to ITS and should be to the individual user as well. They can result in expulsion from the University and federal criminal charges can be assessed.

1.9.5 There will be no dissemination of libelous, slanderous or discriminatory material or any other material as prohibited by law via email or other electronic media.

1.9.6 The Network services including all network wiring, hardware, access points and in-room jacks and physical wiring may not be modified or extended for any reason.

1.10 To make the University’s network as useful, accessible, and effective as possible, there are certain expectations and rules for each user. In addition to common courtesy as network users, these terms of agreement and prerequisites must be adhered to by all users.

1.10.1 Use of the Network services is a privilege and it is the responsibility of each user to utilize these services appropriately. Failure to honor these terms can result in a suspension or loss of networking privileges.

1.10.2 The University’s network is provided with the understanding that it serves primarily as an academic and administrative tool. The University reserves the right to limit or prohibit those activities that might interfere with the network’s academic or administrative use.

1.10.3 A user’s access may be suspended or disabled for violating these terms or provisions of the related policies/conditions/guidelines governing the use of network and computing services at Shawnee State University. Suspensions can also occur if the user’s system is deemed a threat to other computers on the network (e.g., virus infection, security intrusion).

1.10.4 By connecting a host (computer or any other approved device utilizing the network) to the network, users are bound to and required to adhere to all aspects of Policy 5.30Rev. and applicable procedures as well as any and all University, city, county, state and federal regulations, and the network specific rules.

1.10.5 Network access is not permitted for non-affiliates of Shawnee State University without prior guest sponsorship by a university department and approval of IT.

1.10.6 Users may not assign their own IP addresses, change the IP address assigned to them by IT, or manually configure IP addresses.

1.10.7 The network connection may not be used to attempt unauthorized access to any system, or files of any system, or restricted portions of networks to monitor network traffic or to do network routing or serving.

1.10.8 Access to Personal Systems: ITS staff may require access to a user's computer or device to maintain network operations. Users are expected to provide reasonable access to their device and agree to the necessary modifications required to provide network communications and maintain acceptable performance standards.

1.11 Users connecting personal computers and other approved devices to the Network or seeking technical assistance in order to connect computers to the Network understand and agree that Shawnee State University, its contractors, employees, representatives and agents helping the user set up the computer assume no responsibility for a user's loss of time, data or other loss due to unavailable network services or network outages. With full knowledge of the risks involved the user waives any claim whether in tort, contract, or otherwise, for any damage to the user's personal device including but not limited to loss of data, programs, and hardware which may result from technical assistance that is provided by ITS. Furthermore, the user agrees to hold harmless Shawnee State University, its contactors, employees, and agents from any liability of damages the user might incur or cause to others. In addition to this waiver of any claim of damages, the user agrees to assume the risks associated with computer assistance. The user agrees to this waiver, hold harmless agreement and assumption of risk without reservation and certifies that the user has had the opportunity to ask any questions concerning the risks that might be involved with this computer assistance. ITS is charged with ensuring that the users can connect their personally owned devices to the Network. It is at the discretion of the ITS staff the extent to which it will troubleshoot and/or resolve issues related specifically to the equipment.

1.12 The installation of any wireless access device on SSU networks by any individual or group other than ITS is prohibited without prior authorization by the Associate Director of Network & Infrastructure. Any installation must comply with all health, safety, building, and fire codes.

1.13 ITS retains the right to enforce cessation of any unapproved access point, and/or disable network ports where unauthorized access points are found.

1.14 All IP addresses for the SSU Wireless Local Area Network (WLAN) will be assigned and maintained by ITS.

1.15 Installation and Management: ITS will be the sole provider of design, specification, installation, operation, maintenance, and management services for all wireless access points on the SSU Network. The use of other electronic data and telecommunication devices that occupy the same frequency as the SSU WLAN is discouraged on campus. In cases of significant problems, users of other devices will be required to cease using those devices.

1.16 ITS shall resolve frequency conflicts in a manner which is in the best interest of the University and its academic mission.

1.17 Security/Access: It is critical that ITS maintains the necessary security measures consistent with current network practices and protocols. All access points in the SSU WLAN will use a Service Set Identifier (SSID) maintained by ITS. All access points in the SSU WLAN will use authentication and security measures maintained by ITS.

2.0 APPLICATION COMPUTING

Application Computing consists of one or more software programs designed to permit the end user to perform a group of coordinated functions. Application software is installed and operates on Shawnee State University's network and relies on network system software, utilities and resources to provide technology services to the end user. It includes the database management systems and data that are created, stored and transmitted on a daily basis to serve administrative, academic and research functions, operations, and mission of the University.

2.1 All data derived within SSU's enterprise software using campus-wide and departmental-specific applications are considered application computing. Web applications and internet- based technologies operating on the University's network that require the execution of an internet browser during operation are considered application computing.

2.2 ITS maintains sole responsibility for the installation, management and operation of software applications operating as a service on SSU's network. ITS maintains operational and performance standards for quality of service on the network and publishes minimum operating requirements for applications installed on one or more PC clients, or group of computers operating within a computer lab or office on campus.

2.3 Departmental managers and directors may authorize the implementation of application software on the University's network and have the responsibilities of meeting all vendor contractual terms, approvals, obligations and license compliance, and securing the necessary resources required by the application to operate on the network. ITS will advise departments on the conditions for meeting network prerequisites, and any necessary technology commitments and expenses, if applicable.

2.4 Software As A Service: Departments who select application software and/or platform as a service (SaaS/PaaS/Cloud service) as a preferred application provider are responsible for ensuring that all vendor obligations, budget obligations, license compliance and functional administration are met. For any applications that will integrate with current SSU network resources, or that share data and/or processes, managers and directors are responsible to work with ITS to define the scope of integration and requirement of ITS resources to develop and maintain the service.

2.5 Shawnee State email is designated as the primary means for distributing critical information to University employees. Unless otherwise provided in collective bargaining agreements or University policies, communication to University staff and faculty by University officials via campus email constitutes “notice” to the recipients.

2.6 Mass distribution of messages is permissible only for University business and official University sponsored activities.

2.7 Email Access - A University email account may be accessed without the user’s permission upon authorization from a Senior Executive (as defined in 1.3), for any employee placed on temporary or extended leave of absence or who otherwise is not reasonably available in order to secure documents or communications essential to the University mission, or when needed by the office of General Counsel for a legal proceeding.

2.8 ITS will ensure users are aware of the laws in effect to combat unauthorized distribution of copyrighted materials, the steps needed to protect individuals from potential civil and criminal liabilities, and what constitutes a violation of federal copyright laws.

2.9 Software and other materials that are protected by copyright, patent, trade secret, or another form of legal protection ("Protected Materials") may not be copied, altered, transmitted, or stored using SSU-owned or operated technology systems, except as permitted by law or by contract, license agreement, or express written consent of the owner of the Protected Materials. The use of software on a local area network or on multiple computers must be in accordance with the software license agreement.

History
Effective: 06/21/2024