PROCEDURE TITLE:	CONDITIONS FOR USE OF UNIVERSITY COMPUTING RESOURCES
PROCEDURE NO.:	5.30:1
RELATED POLICY:	5.30REV
RESPONSIBLE ADMINISTRATOR(S):	CIO
EFECTIVE DATE:	03/13/2020
NEXT REVIEW DATE:	03/2023
APPROVED BY:	PRESIDENT/VPF&A

These *Conditions for Use* provide comprehensive details that serve as standard operating procedures for three major information technology areas: Section 1: Network Security; Section 2: Network Access; and Section 3: Application Computing. Additional sections may be incorporated to respond to modern technology processes and the delivery of new systems capabilities.

The information describes the conditions for users to gain access and authorized use of Shawnee State University's information technology systems, network, and applications. These conditions incorporate rules and regulations that cover a broad range of technology matters. Users are responsible for understanding and complying with these *Conditions for Use*. They are designed to protect Shawnee State's computing systems from unauthorized access and electronic attacks and to safeguard the University and users.

SECTION 1: NETWORK SECURITY

Information Security is critical to the interests of the University and the many constituencies it serves. As a result of the University's dependency on electronic information, information and information systems must be protected from unauthorized access and electronic attacks to ensure the University can operate without interruption. Priority objectives are safeguarding Institutional Data and protecting confidential information from unauthorized access.

1.0 DEFINITIONS

1.1 Institutional Data: Includes information created, collected, maintained, stored or managed by the University's staff and agents working on the University's behalf. It includes data for the administrative, academic and research functions, operations, and mission of the University. All data derived within the University's enterprise and departmental systems, including but not limited to: Oracle, Jenzabar, Blackboard, FEITH and Cognos applications are considered Institutional Data. Data stored in Microsoft Azure cloud services storage is considered institutional data.

1.1.1 Institutional data do not include personal data created, collected, maintained, transmitted, or recorded on University-owned resources that are not related to University business.

1.2 Confidential Information: Includes information covered and with restrictions governed by laws, such as: FERPA, HIPAA, GLBA, GDPR, PCI, Ohio Revised

Code and other regulatory requirements (e.g., Red Flag rules), and is not releasable to the public under state or federal law. These restricted data could reasonably be used to perpetrate identity theft, constitute a serious and unwarranted invasion of personal privacy, compromise the physical security of University employees or property, or compromise the University's computer systems. Examples of "Confidential Information" include but are not limited to the following:

1.2.1 "Personal information" includes an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable: social security number, driver's license number or state identification card number, account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.

1.2.2 "Personal Financial Information" that links an individual with nonpublic information about that individual's tax return, gross income, investments, financial aid, etc. Note: A public employee's salary is not "personal financial information."

1.2.3 Educational Records: "Any record with certain exceptions, maintained by an institution that is directly related to a student or students. This record can contain a student's name, or students' names, or information from which an individual student or students can be individually identified that include: files, documents, and materials in whatever medium (handwriting, print, tapes, disks, microfilm, microfiche, etc.) that contain information directly related to students and from which students can be personally identified.

1.2.4 "Medical Treatment Records" as defined under state and federal law. The HIPAA Privacy Rule defines protected health information (PHI) as individually identifiable health information, held or maintained by a covered entity (e.g., Shawnee State's group health plan) or its business associates acting for the covered entity, that is transmitted or maintained in any form or medium (including the individually identifiable health information of non-U.S. citizens). This includes identifiable demographic and other information relating to the past, present, or future physical or mental health or condition of an individual, or the provision or payment of health care to an individual that is created or received by a health care provider, health plan, employer, or health care clearinghouse.

1.2.5 Security and Infrastructure records include records or information concerning the protection of a University office against sabotage or attack.

1.2.6 Information that would allow unauthorized access to University computer systems or electronic files.

2.0 DEPARTMENTAL AUTHORITY AND RESPONSIBILITIES

2.1 The department of Information Technology Services (ITS) has overall responsibility for the security of the University's information systems. Implementation of and adherence to security guidelines and best practices to protect confidential information and Institutional Data are the responsibility of all University users.

2.2 All academic and administrative unit managers/directors have the primary responsibility and authority to ensure their respective departments comply with University requirements for privacy and security of specific types of confidential information (e.g., student education records, personnel records, health records, and financial transaction data). These unit managers/directors are responsible for general security issues (e.g., legal issues, security compliance, physical security and communications) as well as for completing risks assessments and assisting in the development of University IT security policies, standards and best practices in the areas of their responsibility.

2.3 Officially protected or confidential information created or maintained by the University including student academic records may reside only on systems or networks operated and maintained by the Department of Information Technology Services (ITS) or contracted vendors unless prior written authorization is given by the University’s Chief Information Officer (CIO).

2.4 Upon recommendation of the CIO, the President or designee, may authorize other networks solely for academic purposes which do not come under the supervision of ITS, provided the department understands its responsibility for the security of such networks under its domain of control and responsibility, and may not use the network to host officially protected or confidential information. These responsibilities include but are not limited to responsibility for general security issues, e.g., legal issues, security compliance and reporting, physical security, communications, and IT infrastructure security on wired and wireless networks. Authorization may be revoked if it is determined that the network is operating contrary to University policy or the law.

3.0 INDIVIDUAL USER RESPONSIBILITIES TO PROTECT INSTITUTIONAL DATA:

3.1 The University’s Institutional Data is a valuable asset and must be maintained and protected as well as remain in compliance with University records retention rules. Further, the privacy of University employees’ personal information as defined as Institutional Data must be protected to the greatest possible extent.

3.2 University employees are assigned roles that require access to Institutional Data in support of the University's teaching, research, and operational objectives. Those employees who use stored Institutional Data during the normal course of business have the responsibility to comply with all state and federal mandates and other applicable laws. These employees are responsible to abide by University guidelines and policies that protect University Institutional Data as well.

3.3 Individuals who use University or personally-owned devices to access University resources are responsible for the security of Institutional Data originating on or downloaded to the mobile device and are subject to guidelines for reporting lost/stolen confidential or Institutional Data, and any associated University-owned data storage device found at https://www.shawnee.edu/areas-study/clark-memorial-library/information-technology-services/information-security/breach-or

4.0 CONDITIONS

4.1 Adherence to the *Conditions for Use* is necessary to protect the University's Institutional Data from accidental or intentional unauthorized access, damage, alteration or disclosure while preserving the ability of authorized users to access and use Institutional Data for authorized University purposes.

4.2 Emailing Stored Institutional Documents

4.2.1 All electronic documents stored within the University-approved database are considered institutional documents, comprised of Institutional Data necessary for University business and potentially confidential and protected information.

4.2.2 Emailing electronic documents created within the University-approved storage databases, to other University employees is permissible using University email and the user's authorized network account access.

4.2.3 Emailing Institutional Data to third-party email systems is not permissible without prior written permission from the direct administrative supervisor.

4.3 Remotely Accessing Confidential Data

4.3.1 Individuals who need remote access to the University's computer network from off-campus require written authorization from the President or Vice President of their respective division. Upon approval, ITS will establish a secure connection to the user's desktop computer. The user is responsible for insuring that data accessed remotely are secured and protected from unauthorized access. Additionally, ITS recommends:

4.3.1.1 Remote access to SSU-managed computing resources is enabled by securely connecting an approved user device to the user's University-managed office computer.

4.3.1.2 Adherence to multi-factor authentication implemented by ITS as a condition of remote access.

4.3.1.3 The user acknowledges in writing to his/her supervisor these conditions and associated responsibilities of the remote access granted to him/her.

4.4 Secured Storage of University Institutional Data

4.4.1 Electronic files with student or employee confidential information or Institutional Data should not be locally (C: drive) stored, stored on departmental Web-shared spaces, or stored on unapproved third-party internet storage mediums. If departmental files need to be locally accessible, a request for a department share should be forwarded to Help_Desk@Shawnee.edu to ensure appropriate security access protocols are established in advance.

4.4.2 Any use of "Cloud" services for storing University Institutional Data or confidential information should be reviewed and approved by ITS prior to such usage.

5.0 SECURITY VIOLATIONS

5.1 Reporting suspected violations of prohibited actions or behavior is the responsibility of all members of the University community.

5.2 Prohibited (actual or attempted) behaviors include but are not limited to:

5.2.1 Allowing institutionally or personally-owned devices with officially protected or personal confidential information to leave the campus without prior written authorization by the departmental supervisor and reasonable efforts by ITS to apply campus-standard security technologies and protocols on the device.

5.2.2 Allowing others to use your personal accounts to access any SSU computing resource or network.

5.2.3 Any attempt involving campus-computing resources for the purpose of hacking. Hacking is defined as attempting (either successfully or unsuccessfully) to break into or gain unauthorized access or rights on a computer system or network. Any unauthorized attempts to access non-university systems will be reported to the administrators of these non-university systems.

5.2.4 Accessing or using a protected computer account assigned to another person or the unauthorized sharing of a password to a protected account with another person without prior authorization by the CIO.

5.2.5 Misuse or abuse of computer equipment, networks, software, or peripheral devices.

5.2.6 Any act which interferes with the appropriate access rights of others.

5.2.7 Transmitting or posting fraudulent, defamatory, harassing, obscene, or threatening messages, or any communications prohibited by law.

5.2.8 Use of any computer network for a purpose contrary to the stated purpose of that network.

5.2.9 Software theft or piracy, data theft, or any other action which violates the intellectual property rights of others.

5.2.10 Deletion, examination, copying, or modification of files and/or data belonging to other users without their prior consent.

5.2.11 Forgery (or attempted forgery) of electronic mail messages.

5.2.12 Deliberate interference with the ability of other users to send/receive electronic mail.

5.2.13 Installation of departmental or enterprise systems intended to support the University’s mission and operations without prior authorization by ITS.

5.2.14 Unauthorized decryption of system or user passwords and files.

5.2.15 The copying of copyrighted materials, or unauthorized sharing of electronic files (audio/video) or third party software without the express written permission of the owner of the copyright.

5.2.16 Intentional attempts to crash systems or programs to disrupt normal operations.

5.2.17 Any improper or unauthorized attempts to secure a higher level of privilege on University systems.

5.2.18 A physical connection of any computer to any of the University's networks without proper authorization from the appropriate network administrator.

5.2.19 Misrepresenting one's identity or relationship to the University when obtaining or using University computer or network privileges.

5.2.20 Creating, installing, or knowingly distributing a computer virus, "trojan horse", phishing attempt, or other surreptitiously destructive program on any University computer or network, regardless of whether any demonstrable harm results.

5.2.21 Adding, modifying or reconfiguring (without proper authorization) the software or hardware of any University computer or network.

5.2.22 Loading of software on campus computers for the purpose of accessing unauthorized network resources.

5.2.23 Any unauthorized access (or attempted access) of student identifiable data.

5.2.24 Using any University computer or network resources to perpetrate a violation of state or federal law or University policies.

5.3 Reporting a Data Security Breach or Loss of Data

5.3.1 Reporting a perceived incident involving Information Security and the potential loss or breach of University confidential information is the responsibility of all members of the University community. Employees are charged to take immediate action when made aware so that responsible persons can meet the institution's obligation to protect the confidential information and limit the institution's risk of loss.

5.3.2 Immediately complete and submit the form titled *Confidential Information-Data Loss or Breach of Security Incident Notification Report* accessed from https://www.shawnee.edu/areas-study/clark-memorial-library/information-technology-services/information-security/breach-or .

6.0 COMPLIANCE WITH BEST PRACTICES

6.1 Users are required to know and comply with best practices established by ITS, the University, and applicable federal, state, or other regulatory standards. Failure to comply with these practices may result in loss of computing privileges and/or disciplinary action.

6.1.1 Lock down console (using <Ctrl-Alt-Delete> function) when not at user station.

6.1.2 Do not share passwords. Passwords should be complex in nature i.e. uses upper/lower case, numbers, special characters.

6.1.3 Log-off or lock down computer when leaving office for the day.

6.1.4 Lock doors when not in office.

6.1.5 Do not share personal office computers with unauthorized users.

6.1.6 Do not share confidential information via the Internet without a secure connection.

6.1.7 Do not respond to emails phishing for personal or institutional information.

6.1.8 Do not store passwords or usernames in a non-secure location.

6.1.9 Do not allow unauthorized individuals into your office or to access your computer. Request ID information from unfamiliar individuals.

6.1.10 Notify Help_Desk@Shawnee.edu when a student or departmental employee terminates employment with SSU or leaves the department.

6.1.11 Notify Help_Desk@Shawnee.edu when an electronic data transmit process (file transmission or the Internet) is needed to complete a University business function.

6.1.12 Access to the Internet from computers with confidential files stored on the personal office computers local hard drive.

6.1.13 Change passwords to third-party software on a frequent basis, using complex passwords (at least every 90 days or as required by the third-party).

6.1.14 Do not keep paper reports with confidential information in non-secured areas and shred all reports and electronic media when no longer needed. Decommissioning of electronic storage devices requires an evaluation by ITS for stored drives/data that must be destroyed prior to related equipment leaving campus.

6.1.15 Do not download (from the Internet) unauthorized, non-work related software onto your computer (i.e. Screensavers, Pointers, etc).

6.1.16 Do not utilize computing resources to the extent that it negatively impacts normal usage by others.

6.1.17 Respect the privacy of other users and their accounts regardless of whether those accounts are securely protected.

6.1.18 Use only those computing resources you are authorized to use and use them only in the manner and to the extent authorized.

6.1.19 Review SSU's educational and training resources for security awareness at https://www.shawnee.edu/areas-study/clark-memorial-library/information-technology-services/information-security/reducing

SECTION 2: NETWORK ACCESS

7.0 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 University-specific purposes, including the support of University academic needs for delivery of instruction, academic and application research and service missions, University administrative functions and student business, student support, and campus-life activities.

8.0 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. Responsible use of computing resources does not extend to just what is technically possible. Users must abide by all applicable restrictions, whether or not a component of the operating system or network or could be circumvented by technical means.

9.0 APPLICABILITY

9.1 Policy 5.30Rev permits access to computing resources and is applicable to current and previous 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.

9.2 Access to some computer programs and network resources may require a written request. Access to information which is private or confidential may be restricted.

9.3 Employees who leave the institution shall have their account access disabled and then deleted after documents of a departmental nature are identified and appropriately dispositioned. Those employees who have been terminated or have received notification of termination will be restricted from access to the system, unless authorized by the President or President's designee.

9.4 Access to some on-campus computers and to external 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.

9.5 Users given access to University computing resources shall be advised of their domain (resources authorized for their use). Users may not go beyond or attempt to go beyond their respective domain without authorization.

9.6 The installation/execution of games and/or recreational programs and devices on Shawnee State systems excluding those required for academic coursework in designated labs and classrooms intended for gaming, is prohibited.

9.7 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 without prior written consent from the Office of the General Counsel.

10.0 Access to University Networks (wired and wireless)

10.1 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.

10.2 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 system, the owner of that computer will be notified of the action taken to resolve the problem.

10.2.1 If the action results in the disconnection of that user from the network, s/he 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 his/her 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.

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

10.3.1 No servers of any kind will be allowed on the network.

10.3.1.1 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.

10.3.1.2 Personal computing devices are not permitted to act as a service provider on the SSU Network.

10.3.1.3 File sharing applications, web servers, gaming servers, including native operating system file sharing services are not permitted.

10.3.2 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.

10.3.3 Network attacks of any kind will not be tolerated.

10.3.3.4 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 charges can be assessed.

10.3.3.5 There will be no dissemination of libelous, slanderous or racist material, or other material prohibited by law.

10.3.4 Software and hardware devices specifically prohibited by the University and ITS will not be permitted on the Network. Devices include network products (e.g. Apple Airport), thin-clients, hubs, switches, routers, print servers, and network appliances.

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

11.0 Terms of Agreement

11.1 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.

11.2 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.

11.3 The University's network is provided with the understanding that it serves primarily as an academic tool. Except for the student residential portion of the network, the University reserves the right to limit or prohibit those activities that might interfere with the network's academic or administrative use.

11.4 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).

11.5 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 Conditions for Use of Campus Computing Resources as well as any and all University, city, county, state and federal regulations, and the network specific rules.

11.6 Network access is not permitted for non-affiliates of Shawnee State University without prior Guest approval by a supporting University department.

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

11.8 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.

11.9 Access to Personal Systems: ITS staff may require access to a User's computer or device to maintain network operations. User agrees to provide reasonable access to their machine and to the necessary modifications required to provide network communications and maintain acceptable performance standards.

11.10 Network Access Prerequisites:

11.10.1 To successfully connect to the Network, each User must first install the required software on their computer. ITS uses Network Access Control technology to ensure that current MS Windows updates and the required anti-virus/anti-malware software are properly installed and running. To continue Network access users must ensure that they have properly configured their computer to receive the latest definition files for each required product. Failure to comply with these prerequisites will result in disconnection from the network until all prerequisites are met.

11.10.2 For other devices that have been approved to connect to the network refer to the Gaming Consoles document posted on the ITS web site.

11.10.3 Periodic Host Scans:

11.10.3.1 ITS reserves the right to perform periodic host scans to ensure there are no vulnerabilities on computers connected to the Network.

11.10.3.2 If a computer is found vulnerable the User will be contacted and advised to make the necessary corrections within a specified time period. If the vulnerability is severe the User will be temporarily disconnected until corrective action is taken.

11.11 Responsibility for All Users: Users are ultimately responsible for any and all network use or communication traffic originating from their personally-owned computer/devices, regardless of the actual author of such traffic.

11.12 Disclaimer of Liability:

11.12.1 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 assumes 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 including but not limited to loss of data, programs, and hardware which may result from work, as well as suggested or required downloads on the User's personal computer. 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 trouble shoot and/or resolve issues related specifically to the equipment.

12.0 Conditions for Wireless Installation and Usage

12.1 To guide the deployment and usage of wireless networking on the SSU campus, to protect the security of SSU's information resources and electronic communications as well as to abate possible interference in the FCC unlicensed 2.4 GHz and 5 GHz radio frequency spectrum, Conditions for Wireless Installation and Usage serve as a prerequisite to implementing and using wireless networks on the SSU campus.

12.2 Installing Personal Wireless Access Points

12.2.1 The installation of any wireless access device on SSU networks by any individual or group other than University Information Services (ITS) is

prohibited without prior authorization by the Chief Information Officer. Any Installation must comply with all health, safety, building, and fire codes.

12.2.2 Students may not install or operate wireless local area network (LAN) access points in the residence halls or any other areas on campus.

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

12.2.4 All IP addresses for the SSU WLAN will be assigned and maintained by ITS.

12.2.5 Acceptable Technology: The Institute of Electrical and Electronic Engineers (IEEE) is responsible for defining and publishing telecommunications and data communications standards. ITS will use these standards as a basis for establishing and keeping current its wireless protocols for the campus.

12.2.6 Installation and Management: University Information Services (ITS) will be the sole provider of design, specification, installation, operation, maintenance, and management services for all wireless access points on the SSU Network. Departments wanting WLAN capability will schedule with ITS for installation and maintenance.

12.3 Radio Signal Interference

12.3.1 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.

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

12.4 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 Information Technology Services. All access points in the SSU WLAN will use authentication and security measures maintained by ITS.

SECTION 3: APPLICATION COMPUTING

13.0 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'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 ad transmitted on a daily basis to serve administrative, academic and research functions, operations, and mission of the University.

14.0 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 requires the execution of an internet browser during operation is considered application computing.

15.0 Information Technology Services 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 on campus. A catalog of managed server-based applications and services maintained by ITS is published on the SSU web site.

16.0 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, any necessary technology commitments and expenses if applicable.

17.0 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 all vendor obligations, budget obligations, license compliance and functional administration are met. For any applications that will integrate with current SSU network resources, 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.

18.0 Campus Email

18.1 The campus unified communications system 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.

18.2 Official University business communications to students is delivered through the Official Notifications portal on the MyInfo tab, within MySSU, and via campus email sent by the student business areas or the Office of Communications. Any communication sent from student business units to the Official Notifications portal on the MyInfo tab within MySSU, constitutes "notice" to the recipients.

18.3 Intended Recipients - Electronic mail (email) is intended for communication between individuals and clearly identified groups of interested individuals, not for mass distribution.

18.4 Mass Distribution is defined as sending an email to a group of University users, who have not otherwise indicated their desire to receive messages that are not directly related to their University position or the University's mission. Sending multiple copies of the same message to multiple groups is also mass distribution. Mass distribution of messages is permissible only for University business and official University-sponsored activities. Mass distribution of other non-University business and non-University-sponsored activities may be considered "spamming" and a violation of the Conditions for Use of Campus Computing Resources as determined by the President or President's designee.

18.5 Email Access - A University email account may be accessed without the user's permission upon authorization from the President or Vice President of their respective division, for any employee placed on temporary or extended leave of absence, or otherwise is not reasonably available in order to secure documents or communications essential to the mission.

19.0 Software Use and Intellectual Property Rights

19.1 Shawnee State is committed to educating its students, faculty and staff on the importance of understanding its role as an institution of higher education and the regulations it must adhere to as defined within the Higher Education Opportunity Act (HEOA). Combating the unauthorized distribution of copyrighted materials by users of the Shawnee State network, without interfering with the purpose of educational and research use of the network, is an overall goal of ITS.

19.2 It is the University's shared responsibility to protect the institution from copyright infringement. Overall campus awareness, policy enforcement and technology are all deterrents that comprise safeguards in place to protect students, faculty and staff. Each of us needs to be aware of the laws in effect to combat unauthorized distribution of copyrighted materials, and the steps needed to protect individuals from potential civil and criminal liabilities, and disciplinary action for violation of federal copyright laws.

19.3 ITS understands its role in accepting the responsibility to implement industry-standard technologies that deter copyright infringement and actively monitors traffic on the network for unauthorized use and distribution of content, and responds to any notice from an authority charged to protect copyrighted material as reported under the Digital Millennium Copyright Act (DMCA).

19.4 Respect for the scholarly work and intellectual property rights of others is essential to the educational mission of any University. Shawnee State University, therefore,

endorses the following 1987 EDUCOM/ADAPSO statement on *Software and Intellectual Rights*:

"Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgement, right to privacy, and right to determine the form, manner, and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against the violator."

19.5 Protecting Against Copyright Infringement

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: 03/13/2020