Oklahoma State University - Oklahoma City
Policy and Procedures

Technology Policy	**1-6003** **General University Policy**

Executive Summary

Use of University information technology systems in any way contrary to applicable Federal or State statutes or the policies of Oklahoma State-University Oklahoma City (OSU-OKC) is prohibited. State law prohibits the use of university equipment, supplies or other resources for personal business or benefit. Disciplinary actions may result in loss of privileges, immediate termination, and potentially leading to criminal penalties.

Under Oklahoma law, all electronic mail messages are presumed to be public records and contain no right of privacy or confidentiality except where Oklahoma or Federal statutes expressly provide for such status. The University reserves the right to inspect electronic mail usage by any person at any time without prior notice as deemed necessary to protect the University to the full extent not expressly prohibited by applicable statutes.

Appropriate OSU-OKC employees are provided with all the necessary computer equipment, access, and software to perform their assigned duty. Information Technology (IT) staff will review and inventory all purchases of computer equipment and software. All computing software, peripherals and associated hardware must be approved by IT.

Appropriate Technology Use

1 Purpose

As an institution of higher learning, OSU-OKC(University) encourages, supports, and protects freedom of expression and an open environment to pursue scholarly inquiry and to share information. Access to networked computer information in general and to the Internet, in particular, supports the academic community by providing a link to electronic information in a variety of formats and covering all academic disciplines. Consistent with other University policies, this policy is intended to respect the rights and obligations of academic freedom, while protecting the rights of others. The computing, technology and network facilities of the University are limited and should be used wisely and carefully with consideration for the needs of others. As with any resource, it is possible to misuse computing resources and facilities and to abuse access to the Internet.

2 Scope

This policy is applicable to all individuals using University owned or controlled information technology facilities, equipment and network, whether such persons are students, staff, faculty, or authorized third-party users of University information technology resources. It is applicable to all University information technology resources whether individually controlled or shared, stand alone or networked. It applies to all information technology facilities, and equipment owned, leased, operated, or contracted by the University. This includes, but is not limited to, desktop and laptops computers, cell phones, and associated devices, online services, software, and electronic mail accounts, regardless of whether used for administration, research, teaching, or other purposes.

3 User Responsibilities and Expectations

A. Access to information technology resource infrastructure both within and beyond the University campus, sharing of information and security of the intellectual products of the community all require that each and every user accept responsibility to protect the rights of the community. Access to the networks and to the information technology resources at OSU-OKC is a **privilege** granted to University **students, faculty, staff, and third parties** who have been granted special permission to use such facilities. Access to University information resources must take into account the following factors: relevant laws and contractual obligations, the requestor's need to know, the information's sensitivity, and the risk of damage to or loss by the University.

B. Anyone who accesses, uses, destroys, alters, or damages University information resources, properties, or facilities without authorization, may be guilty of violating state or federal law, infringing upon the privacy of others, injuring or misappropriating the work produced and records maintained by others, and/or threatening the integrity of information kept within these systems. Such conduct is unethical and unacceptable and will subject violators of this Policy to disciplinary

action by the University, including possible termination from employment, expulsion as a student, and/or loss of computing systems privileges.

C. The University reserves the right to limit, restrict, or extend computing privileges and access to its information resources. Data owners—whether departments, units, faculty, students, or staff—may allow individuals other than University faculty, staff, and students access to information for which they are responsible, so long as such access does not violate any license or contractual agreement, University policy, or any federal, state, county, or local law or ordinance. However, users are personally responsible for all activities on their user-id or computer system and may be subjected to disciplinary action and/or loss of privileges for misuse of computers or computing systems under their control even if not personally engaged in by the person controlling the computer or system.

D. Units and individuals may, with the permission of the appropriate University officials and in consonance with applicable University policies and guidelines, configure computing systems to provide information retrieval services to the public at large. However, in so doing, particular attention must be paid to University policies regarding authorized use (must be consistent with the mission of the University), ownership of intellectual works, responsible use of resources, use of copyrighted information and materials, use of licensed software, and individual and unit responsibilities.

3.1 Authorized User

A. Use of University computers must comply with Federal and State law and University policies. University computing facilities and accounts are to be used for the University-related activities for which they are assigned. When users cease to be members of the academic community (such as by graduating or ceasing employment), or when persons are assigned to a new position and/or responsibilities within the University, the access authorization of such person will be reviewed and may be altered. Users whose relationships with the University change may not use computers and computing resources, facilities, accounts, access codes, privileges, or information for which they are not authorized in their new relation to the University.

B. Users may use only their own computer accounts. The negligence or naiveté of another user in revealing an account name or password is not considered authorized use. Convenience of file or printer sharing is not sufficient reason for sharing a computer account. Users are personally responsible for all use of their computer account(s).

C. Appropriate use of computing and networking resources includes instruction, independent study, authorized research, independent research, communications, and official work of the offices, units, recognized student and campus

organizations, and agencies of the University. Computing facilities, services, and networks may not be used in connection with compensated outside work for the benefit of organizations unrelated to the University unless authorized. Computing and network facilities for personal gain or profit, and use of computing resources for unauthorized commercial purposes, unauthorized personal gain, or any illegal activities is prohibited.

3.2 Special User Notifications

A. The University makes available both internal and external computing facilities consisting of hardware and software. The University accepts no responsibility for any damage to or loss of data arising directly or indirectly from the use of these facilities or for any consequential loss or damage. The University makes no warranty, express or implied, regarding the computing services offered, or their fitness for any particular purpose.

B. The University cannot protect individuals against the existence or receipt of material that may be offensive to them. As such, those who make use of electronic communications are warned that they may come across or be the recipients of materials they find offensive. Those who use e-mail and/or make information about themselves available on the Internet should be forewarned that the University cannot protect them from invasions of privacy and other possible dangers that could result from the individual's distribution of personal information.

C. An individual using University computing resources or facilities must do so in the knowledge that usage of University resources are in support of work or academic pursuit. The University has the right of access to the contents of stored computing information at any time for any purpose for which it has a legitimate "need to know." The University will make reasonable efforts to maintain the confidentiality of computing information storage contents and to safeguard the contents from loss but is not liable for the inadvertent or unavoidable loss or disclosure of the contents.

D. Any individual using University computing resources and facilities must realize that all computer systems maintain internal audit trials logs or file logs. Such information as the user identification, date and time of the session, the software used, the files used, the computer time, and storage used, the user account, and other related information is normally available for diagnostic, accounting, and load analysis purposes. Under certain circumstances, this information is reviewed by system administrators, either at the request of an academic department, or in situations where it is necessary to determine what has occurred to cause a particular system problem at a particular time. For example, analysis of audit files may indicate why a particular data file is being erased, when it was erased, and what user identification has erased it.

E. OSU-OKC IT employees and system administrators do not routinely look at individual data files. However, the University reserves the right to view or scan any file or software stored on the computer or passing through the network and will do so periodically to verify that software and hardware are working correctly, to look for particular kinds of data or software (such as computer viruses), or to audit the use of University resources. Violation of policy that comes to the attention of University officials during these and other activities will be acted upon. User data on the computing systems will be periodically copied to backup media. The University cannot guarantee confidentiality of stored data. Users should be aware that use of one of the data networks, such as the Internet, and electronic mail and messages, will not necessarily remain confidential from third parties outside the University in transit or on the destination computer system, as those data networks are configured to permit fairly easy access to transmissions.

3.3 Conduct Expectations and Prohibited Actions

A. The well-being of all OSU-OKC operations depends on the availability and integrity of the system. Any defects discovered in the system accounting or system security are to be reported to the appropriate system administrators so that steps can be taken to investigate and solve the problem. The cooperation of all users is needed to ensure prompt action. The integrity of most systems is maintained by password protection of accounts. A computer user who has been authorized to use such a protected account may be subject to both criminal and civil liability, as well as University discipline, if the user discloses a password or otherwise makes the account available to others without the permission of the system administrator.

B. Restrictions on computer security and self-replicating code are to be interpreted in a manner that protects university and individual computing environments but does not unduly restrict or limit legitimate academic pursuits.

C. The following examples of acts or omissions, though not covering every situation, specify some of the responsibilities that accompany computer use at OSU-OKC, and outline acts or omissions that are considered unethical and unacceptable, and may result in immediate revocation of privileges to use the University's computing resources and/or just cause for taking disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action.

    i. Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization. Software protected by copyright shall not be copied except as specifically stipulated by the owner of the copyright. Protected software is not to be copied into, from, or by any University facility or system, except by license. The number and distribution of copies must be handled in such a way that the number of simultaneous users in a department does not exceed the number of original copies licenses or seats

purchased by that department, unless otherwise stipulated in the purchase contract.

ii. Interfering with the intended use of the information resources or without authorization, destroying, altering, dismantling, disfiguring, preventing rightful access to or otherwise interfering with the integrity of computer-based information and/or information resources.

iii. Modifying or removing computer equipment, software, or peripherals without proper authorization.

iv. Encroaching on others' use of the University's computers. This includes but is not limited to: the sending of non-business related chain-letters or excessive messages, either locally or off-campus; printing excess copies of documents, files, data, or programs; running grossly inefficient programs when efficient alternatives are known to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a University computer; damaging or vandalizing University computing facilities, equipment, software, or computer files.

v. Developing or using programs which harass other computer users or which access private or restricted portions of the system and/or damage the software or hardware components of the system. Computer users shall use great care to ensure that they do not use programs or utilities which interfere with other computer users or which modify normally protected or restricted portions of the system or user accounts. The use of any unauthorized or destructive program may result in legal civil action for damages or other punitive action by any injured party, including the University, as well as criminal action.

vi. Using University computing resources for commercial purposes or non-University-related activities without written authorization from the University. In these cases, the University will require restitution payment of appropriate fees. This Policy applies equally to all University-owned or University-leased computers.

vii. Using University computing resources to generate or access obscene material as defined by Oklahoma or federal law and acceptable community standards or creating a hostile work and/or educational environment.

viii. Seeking to gain or gaining unauthorized access to information resources or enabling unauthorized access.

ix. Accessing computers, computer software, computer data or information, or networks without proper authorization, or intentionally allowing others to

do so, regardless of whether the computer, software, data, information, or network in question is owned by the University. For example, abuse of the networks to which the University belongs or the computers at other sites connected to those networks will be treated as an abuse of OSU-OKC computing privileges.

x. Without authorization invading the privacy of individuals or entities that are creators, authors, users, or subjects of the information resources.

xi. Using University electronic communication facilities to send fraudulent, harassing, obscene, threatening, or other unlawful messages is prohibited. Users shall respect the purpose and charters of computer mailing lists (including local or network news groups and bulletin-boards). It is the responsibility of any user of an electronic mailing list to determine the purpose of the list before sending messages to the list or receiving messages from the list. Persons subscribing to an electronic mailing list will be viewed as having solicited any material delivered by the list as long as that material is consistent with the purpose of the list. Persons sending to a mailing list any materials which are not consistent with the purpose of the mailing list will be viewed as having sent unsolicited material to the mailing list.

xii. Transmitting commercial or personal advertisements, solicitations, promotions, or programs intended to harass other computer users or access private or restricted computer or network resources.

xiii. Seeking to provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users without the permission of those other users; Using programs or devices to intercept or decode passwords or similar access control information.

xiv. Attempting to circumvent mechanisms intended to protect private information from unauthorized examination by others in order to gain unauthorized access to the system or to private information; Configuring or running software so as to allow unauthorized use.

xv. Using University computers or computing systems in any manner which violates Federal, state, or local laws, or University policies.

xvi. Using University computing facilities or accounts for other than the University-related activities for which they were assigned and intended.

xvii. Using computers or the University computing resources to engage in political campaigning or commercial advertisement.

3.4 System Administrator Responsibilities

A. The **Board of Regents** for Oklahoma State University and the Agricultural and Mechanical Colleges are the **legal owners of all** University "owned" or controlled **computers, networks, and related information technology devices**. The contents of all storage media owned or stored on University computing facilities are the property of OSU-OKC .

B. Management of the data which is contained within the various data systems of the University must be administered in a fashion consistent with the mission and efficient operations of the University, applicable state or federal laws, and potentially applicable privacy considerations.

C. User access and file control is maintained by the IT is the primary resource for resolving questions about internal user access rights. Users and administrators of the various computing system components owned or controlled by the University are required to follow those internal management guidelines. Failure to comply with those guidelines can result in disciplinary and/or legal action.

D. The system administrator has certain responsibilities to the University as a whole for the system(s) regardless of the policies of the department or group, and the owner has the ultimate responsibility to see that these are carried out by the system administrator. These responsibilities are:

   i. To take reasonable precautions against theft of, or damage to, the system components.

   ii. To faithfully execute all hardware and software licensing agreements applicable to the system.

   iii. To treat information about, and information stored by, the system's users as confidential (as conditioned in this policy) and to take reasonable precautions to ensure the security of a system or network and the information contained therein.

E. The system administrator is authorized to take all reasonable steps and actions to implement and enforce the usage and service policies of the system and to provide for security of the system. System administrators operating computers and networks may routinely monitor and log usage data, such as network session connection times and end-points, CPU and disk utilization for each user, security audit trails, network loading, etc. These units may review this data for evidence of violation of law or policy and for other lawful purposes. System administrators may access computer user' files at any time for maintenance purposes. System administrators may access other files for the maintenance of networks and computer and storage systems, such as to create backup copies of media.

F. When system response, integrity, or security is threatened, a system administrator is authorized to access all files and information necessary to find and correct the problem or otherwise resolve the situation.

G. If an occasion arises when a University officer or supervisor believes that access to an individual's data is required for the conduct of University business (unrelated to the need to investigate possible wrongdoing), the individual is not available, and a system administrator is required to access the individual's account, the following procedure shall be followed:

   i. The University official or supervisor shall secure documented permission to access the data from the Direct Supervisor, Vice President for Operations Director of Human Resources and CIO.

H. System administrators are required to report suspected unlawful or improper activities to the CIO. Computer users, when requested, have an affirmative duty to cooperate with system administrators in investigations of system abuse. Users are encouraged to report suspected illegal activity or abuse, especially if related to any damage to or problems with their files.

I. If an occasion arises when a University officer or supervisor believes that a user is violating state or federal law, or University policy, and that access to an individual's data is required in order to conduct an internal investigation into such possibility, system administrators may monitor all the activities of and inspect the files of such specific user(s) on their computers and networks.

J. A review of user access rights will be conducted twice a year in order to ensure that all usage and access to information systems conforms to the principle of least privilege.

4 Enforcement

A. Users are expected to fully cooperate with system administrators in any investigations of system abuse. Failure to cooperate may be grounds for cancellation of access privileges or disciplinary action.

B. Abuse of computing privileges is subject to disciplinary action. If system administrators have strong evidence of misuse of computing resources, and if that evidence points to the computing activities or the computer files of an individual, they have the obligation to pursue any or all of the following steps to protect the user community:

   i. Suspend or restrict the user's computing privileges during the investigation.
   ii. Inspect the user's files, disks, and/or other computer-accessible storage media. System administrators must be certain that the trail of evidence

clearly leads to the user's computing activities or computing files before inspecting the user's files.

iii. Refer the matter for possible disciplinary action to the appropriate University department leadership.

C. Individuals whose privileges to access University computing resources have been suspended may request that the Vice President for Operations, or designee, review the suspension. In consultation with the Vice President for Operations, or designee may reinstate privileges, alter any restrictions that have been imposed, or refuse to interfere with the administrative action taken to that time.

5 Network Security

A. The OSU-OKC computer network exists to facilitate the operations, education mission and community outreach of the University. The network provides electronic capabilities that allow OSU-OKC faculty, staff, students or affiliates to access information, share data, collaborate, and communicate. IT manages the network and is responsible for its secure and effective operation. IT is responsible for the maintenance, planning and implementation of network growth and to coordinate these efforts with units and departments.

B. The network consists of the following:

i. **Access-Layer Network Infrastructure** - network wiring and electronics (network switches and/or hubs) in OSU-OKC buildings that interconnect OSU-OKC's computers and other devices.

ii. **Wireless Network Access "Air Space"** - radio spectrum used for wireless network access at OSU-OKC.

iii. **Network Backbone and Building Switches** - top-level network switches/routers in each building and the core OSU network backbone that connect OSU-OKC building networks together and to off-campus networks.

iv. **Wide Area Network Connections** - Wide Area Network (WAN) that connects distributed portions of the OSU-OKC network.

v. **Connections to Regional and National Networks (OneNet)** - off-campus connections to the Internet. OneNet is Oklahoma's telecommunications and information network for education and government. OneNet is a division of the Oklahoma State Regents for Higher Education.

vi. **Core Network Services** - services required for (Domain Name Service, DHCP, WINS, etc.)

vii. **OSU-OKC Network** – the infrastructure to provide data and communication services and resources.

viii. **Eduroam** - (education roaming) is the secure, world-wide roaming wireless service developed for and by the international research and

education community. Eduroam allows students, researchers and staff to roam and find connectivity at more than 2,500 locations in the US, and more than 33,000 worldwide.

ix. **Subordinate Departmental Network** – an independent network whose purpose is to fulfill academic purpose in a limited non-public manner.

C. **OSU-OKC Network as a Principal Institutional System -**The network is a critical campus principal institutional system, available to all faculty, staff, students or affiliates, at all campus locations. It provides end-to-end "wall plate to wall plate" service from any computer on campus to any other, as well as to off-campus computers and resources.

D. **Subordinate Departmental Network -** A departmental network is considered an independent system and **shall not be directly interfaced with any institutional system**

E. **Wireless Network -** Wireless services are subject to the same rules and policies that govern other Information Technology at OSU.

F. **TCP/IP – OSU-OKC's Network Protocol -** To facilitate interoperability among OSU systems, the network backbone currently supports only TCP/IP and other IP based protocols.

G. **Involuntary Disconnection -** To assure the integrity of the network, it may be necessary for IT to disconnect a host, a group of hosts, or a network that is unsecured or disrupting network service to others. This includes hosts involved in network security problems, such as those used by unauthorized parties to attack other systems on the OSU-OKC Network or on the Internet. If the situation allows, IT will make an attempt to contact the local security liaison or owner of the host or hosts involved. If those individuals are not available**,** the disconnection may proceed without notification. With regard to security issues, a disconnection might be a "partial" one that isolates the host from attacking hosts, or from off-campus access in general. A host that has been compromised by unauthorized parties may need to stay disconnected until the host's operating system can be updated and all changes made by the attacker reversed.

H. **Physical Access to Wiring Closets -** Only IT is authorized to place equipment or cabling in wiring closets, equipment rooms, etc.

6 IT Responsibilities

A. **Network Maintenance -** IT maintains building and campus network wiring and fiber, local switches, building routers/switches, backbone routers/switches, and other network devices that comprise the OSU-OKC network. This includes troubleshooting

problems, identifying their cause, and replacing or repairing defective equipment and wiring.

B. **Network Documentation -** IT is responsible for creating and maintaining the detailed documentation of the network required for proper network maintenance, operation, and planning.

C. **Administration of OSU-OKC Network Connections to Other Networks -** IT maintains relationships and agreements with OneNet and other service providers to keep the OSU-OKC Network well connected to the commercial Internet and academic networks. IT administers all interfaces between networks and connections between the OSU-OKC Network and other networks.

D. **Administration of OSU –OKC Network Name and Address Space -** IT manages the network name space and the assignment of names and network addresses (IP numbers) for security and identity of users.

E. **Administration of OSU-OKC Wireless Networking -** IT manages the radio spectrum for use of wireless networking to ensure compatible access to all OSU-OKC users.

F. **Central Network Services -** IT provides central services required for operation of the network.

G. **Network Devices -** The network is a mission-critical strategic University resource. In order to protect the network, devices other than computers, servers, printers, and workstations must be approved as an exception to policy by IT before being plugged into any network port. These devices may be incorrectly configured or incompatible with the OSU-OKC Network causing outages and reliability problems to all or part of the network. Devices not approved for use on Network will be disabled to ensure the stability and availability of the network.

H. **Traffic Monitoring -**IT monitors traffic flow to optimize network usage, detect network problems, and ensure equitable access and other properly authorized investigations.

I. **Security Monitoring -** To the extent possible, IT monitors network traffic to detect the "signatures" of known network intrusion scenarios, viruses, or the like. IT may periodically scan the OSU-OKC network hosts to assess the vulnerability to attack. It should be noted that there is no guarantee that IT will be able to detect all potential system vulnerabilities.

J. **Campus-wide Network Security Coordination -** IT promotes campus-wide network security and coordinates campus-wide response to unauthorized access. This also includes working with local supporters, computer users, and OneNet to protect the campus from network intrusions, denial of service attacks, and other unauthorized and/or inappropriate activities that impair network access and use.

K. **Planning for Network Growth -** IT interacts with campus departments to ensure current and future communication needs are addressed.

L. **Upgrades to Current Infrastructure** - IT performs upgrades to the current infrastructure to ensure current and future needs are addressed. All devices and services that are at end-of-life or unsupported by the vendor shall be discontinued. All software patches and upgrades must be documented reviewed, tested in pre-production and applied in production environments. Any temporary variance to this policy will be documented for audit purposes and isolated to reduce vulnerability.

M. **Systems Security Officer (SSO) –**OSU-OKC's Network Security Analyst (NSA) is designated by the OSU-OKC CIO, is the primary contact to work in conjunction with appropriate OSU and the CIO university officials for the interpretation, enforcement and monitoring of this policy and the resolution of problems concerning it. OSU-OKC complies with NIST 800-53 Standard MA-1. In situations that are an immediate threat to the security or operation of a computer or network, the NSA may require immediate intervention of access privileges and affected user files or messages. In such an emergency, the NSA will immediately notify the appropriate university administrators and users affected by the situation.

N. **Training** – IT is responsible in coordination with Human Resources to provide annual IT security training. Training shall be conducted quarterly in a mixed environment of online or in person format to ensure documented awareness and compliance.

7 Individual or Unit Responsibilities

A. The primary users of technology connected to the OSU-OKC network are responsible for the following:

   i. **Abiding by OSU-OKC's Appropriate Technology Use Policy** - Users should efficiently use network resources and follow OSU-OKC's Appropriate Technology Use Policy Computer and OSU's Network Security Policy. Users are personally responsible for all activities on their User ID or computer system including security of their own passwords and may be subjected to disciplinary action and/or loss of privileges for misuse of computers or computing systems under their control, even if not personally engaged in by the person controlling the computer or system.

   ii. **Reporting Problems** - Users should promptly report network problems to the OKC IT HelpDesk , and cooperate with support staff in correcting malfunctions.

   iii. **Taking Proper Security Precautions -** Users are required to changed passwords every 90 days. Each password will abide by the complexity rules outlined in the OSU Central Administration Services (CAS).

iv. **Keeping the Operating System Secure –** OSU-OKC centrally manages upgrades and patches for computer operating systems.

v. **Special Notifications -** The University's computing and network systems are a university owned resource and business tool only to be used by authorized individuals for business and academic purposes. Users should never distribute mailing lists owned by the University. The University owns everything stored in its systems unless it has agreed otherwise. The University has the right of access to the contents of stored computing information at any time for any purpose for which it has a legitimate "need to know." The University will make reasonable efforts to maintain the confidentiality of computing information storage contents and to safeguard the contents from loss, but is not liable for the inadvertent or unavoidable loss or disclosure of the contents. Devices not approved for use on OSU-OKC's Network will be disabled.

8 Server Security

A. All internal servers deployed at OSU-OKC must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by IT. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by IT.

B. Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
   i. Server contact(s) and location, and a backup contact
   ii. Hardware and Operating System/Version
   iii. Main functions and applications, if applicable

C. Information in the corporate enterprise management system must be kept up-to-date.

D. Configuration changes for production servers must follow the appropriate change management procedures.

E. Changes to the network will be managed in the online management tracker, including accounting for any network security concerns should they arise during planning. The guidelines governing change management are spelled out in the risk and approval matrices document.

8.1 General Configuration Guidelines

A. Operating System configuration should be in accordance with approved IT guidelines. Server must be in the Active Directory OU for servers ad.osuokc.edu/Servers.

B. Services and applications that will not be used must be disabled where practical.

C. Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.

D. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements. In order to receive security updates and patches, servers must be in the ad.osuokc.edu/Servers OU. SCCM has been authorized to automatically apply patches based on the classification of the device. Currently there are three classifications, 1. Non-critical production, 2. Moderate critical production and 3. Critical production. Non-critical production servers are updated the morning after patch Tuesday, moderate critical are updated the night after patch Tuesday and critical production servers are updated the Sunday following patch Tuesday. Versioning shall be recorded and maintained in the IT software library. Testing and updates for domain controllers are performed manually at a time that does not interfere with business requirements. Devices at end-of-patching are to be upgraded to their most recent available software.

E. Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is available.

F. Always use standard security principles of least required access to perform a function.

G. Do not use root, or administrative accounts when a non-privileged account is sufficient.

H. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

I. Servers should be physically located in an access-controlled environment.

J. Servers are specifically prohibited from operating from uncontrolled areas, such as cubicles, or shared offices.

8.2 Monitoring

A. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
   i. All security related logs will be kept online for a minimum of 1 week.
   ii. Daily differential backups will be retained for at least 1 month.
   iii. Weekly full backups of logs will be retained for at least 1 month.
   iv. Monthly full backups will be retained for a minimum of 1 years.

B. Security-related events will be reported to IT, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
   i. Port-scan attacks
   ii. Evidence of unauthorized access to privileged accounts
   iii. Anomalous occurrences that are not related to specific applications on the host.

8.3 Compliance

A. Audits will be performed on a regular basis by authorized organizations within OSU-OKC.

B. Audits will be managed by the internal audit group or IT, in accordance with the *Audit Policy*. IT will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.

C. Every effort will be made to prevent audits from causing operational failures or disruptions.

8.4 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

8.5 Definitions

Term	**Definition**
DMZ	De-militariezed Zone. A network segment external to the corporate production network.
Server	For purposes of this policy, a Server is defined as an internal OSU-OKC Server.

NOTE: Desktop machines and Lab equipment are not relevant to the scope of this policy.

9 Passwords on Accounts and Network Devices

A. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

B. All production system-level passwords must be part of the IT administered global password management database.

C. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.

D. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

E. Passwords must not be inserted into email messages or other forms of electronic communication.

F. Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

G. All user-level and system-level passwords must conform to the guidelines described below.

H. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9.1 Definitions

Terms	Definitions
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

10 Remote Access

A. It is the responsibility of OSU-OKC employees, contractors, vendors and agents with remote access privileges to OSU-OKC's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to OSU-OKC.

10.1 Requirements

A. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.

B. At no time should any OSU-OKC employee provide their login or email password to anyone, not even family members.

C. OSU-OKC employees and contractors with remote access privileges must ensure that their OSU-OKC-owned or personal computer or workstation, which is remotely connected to OSU-OKC's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

D. OSU-OKC employees and contractors with remote access privileges to OSU-OKC's corporate network must not use non-OSU-OKC email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct OSU-OKC business, thereby ensuring that official business is never confused with personal business.

E. Routers for dedicated ISDN lines configured for access to the OSU-OKC network must meet minimum authentication requirements of CHAP.

F. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

G. Frame Relay must meet minimum authentication requirements of DLCI standards.

H. Non-standard hardware configurations must be approved IT, and IT must approve security configurations for access to hardware.

I. All hosts that are connected to OSU-OKC internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.

J. Personal equipment that is used to connect to OSU-OKC's networks must meet the requirements of OSU-OKC-owned equipment for remote access.

K. Organizations or individuals who wish to implement non-standard Remote Access solutions to the OSU-OKC production network must obtain prior approval from IT.

10.2 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

11 Audit

A. To provide the authority for members of OSU-OKC's IT team to conduct a security audit on any system at OSU-OKC.

B. Audits may be conducted to:
   i. Ensure integrity, confidentiality and availability of information and resources
   ii. Investigate possible security incidents ensure conformance to OSU-OKC security policies
   iii. Monitor user or system activity where appropriate.
   iv. Access may include:
      a. User level and/or system level access to any computing or communications device
      b. Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on OSU-OKC equipment or premises
      c. Access to work areas (labs, offices, cubicles, storage areas, etc.)
      d. Access to interactively monitor and log traffic on OSU-OKC networks

C. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any student found in violation of this policy are subject to disciplinary action as outlined in the Student Code of Conduct.

12 Definitions

Term	Definition
Cable Modem	Cable companies such as Cox Communications provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCIData Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay

	network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
ISDN	There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.
Remote Access	Any access to OSU-OKC's corporate network through a non-OSU-OKC controlled network, device, or medium.

13 Revision History

Version	Date	Description	Approved By
1.1	November 21st, 2022	Revised in line with A&M Board of Regents Cybersecurity Audit criteria	Richard Barr; Christian Davis
1.2	July 13, 2023	Revised for OSU-OKC policy format compliance	Mike Widell