

Oklahoma State University-Oklahoma City Technology Policies

Executive Summary.....	3
General Policies (OSU-Oklahoma City Community).....	4
Appropriate Technology Use.....	4
1.0 Purpose	4
2.0 Scope.....	4
3.0 Policy	5
3.1 User Responsibilities and Expectations	5
3.2 Authorized User Purposes	6
3.3 Special User Notifications	7
3.4 Conduct Expectations and Prohibited Actions.....	8
3.5 System Administrator Responsibilities.....	11
4.0 Enforcement.....	14
4.1 Consequences of Misuse of Computing Privileges.....	14
Network Security	15
1.0 Purpose	15
2.0 Scope.....	15
3.0 Policy	16
3.1 OSU-Oklahoma City Network Components.....	16
3.2 General Provisions	17
3.3 IT Responsibilities.....	19
3.4 Division or Department Responsibilities.....	20
3.5 User Responsibilities.....	21
4.0 Enforcement.....	22
Specific Policies (Technology Professionals)	22
Server Security.....	22
1.0 Purpose	22
2.0 Scope.....	23
3.0 Policy	23
3.1 Ownership and Responsibilities.....	23
3.2 General Configuration Guidelines.....	23
3.3 Monitoring.....	24
3.4 Compliance	25
4.0 Enforcement	25
5.0 Definitions.....	25
6.0 Revision History	25
Internal Lab Security.....	25
1.0 Purpose	25
2.0 Scope.....	26
3.0 Policy	26
3.1 Ownership Responsibilities.....	26
3.2 General Configuration Requirements.....	27

- 4.0 Enforcement 29
- 5.0 Definitions 29
- 6.0 Revision History 30
- De-Militarized Zone Lab Security 30
 - 1.0 Purpose 30
 - 2.0 Scope 30
 - 3.0 Policy 30
 - 3.1. Ownership and Responsibilities 30
 - 3.2. General Configuration Requirements 31
 - 4.0 Enforcement 33
 - 5.0 Definitions 33
 - 6.0 Revision History 34
- Passwords on Accounts and Network Devices 34
 - 1.0 Purpose 34
 - 2.0 Scope 34
 - 3.0 Policy 34
 - 3.1 General 34
 - 3.2 Guidelines 35
 - 4.0 Enforcement 37
 - 5.0 Definitions 37
 - 6.0 Revision History 38
- Remote Access 38
 - 1.0 Purpose 38
 - 2.0 Scope 38
 - 3.0 Policy 38
 - 3.1 General 38
 - 3.2 Requirements 39
 - 4.0 Enforcement 40
 - 5.0 Definitions 40
 - 6.0 Revision History 42
- Audit 42
 - 1.0 Purpose 42
 - 2.0 Scope 42
 - 3.0 Policy 42
 - 4.0 Enforcement 42
 - 5.0 Definitions 43
 - 6.0 Revision History 43

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 is prohibited and will make you subject to University disciplinary actions, including possible immediate termination, and may also subject you to criminal penalties. State law prohibits the use of university equipment, supplies or other resources for personal business or benefit.

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 business-related concerns of the University to the full extent not expressly prohibited by applicable statutes.

All new Oklahoma State University-Oklahoma City (OSU-Oklahoma City) employees will be set up with all the necessary computer equipment, access, and software. Information Technology (IT) staff will review and inventory all purchases of personal computer equipment and software. Software or hardware not approved by IT will not be supported.

OSU-Oklahoma City employees should not make copies of software residing on computers for any reason except backup purposes. Software or hardware should not be taken from the OSU-Oklahoma City campus without prior written permission from the supervisor. In addition, personal software or hardware should not be used without prior written permission from the supervisor.

General Policies (OSU-Oklahoma City Community)

Appropriate Technology Use

1.0 Purpose

As an institution of higher learning, OSU-Oklahoma City 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. The following statements address, in general terms, the OSU-Oklahoma City's philosophy about technology use.

2.0 Scope

This policy is applicable to all individuals using University owned or controlled information technology facilities or equipment, 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, laptops, pagers, cell phones, personal digital assistants (PDAs), computers, and associated devices and software, and electronic mail accounts, regardless of whether used for administration, research, teaching, or other purposes. The University policy regarding Access by External Users and any subsequent revisions thereto may apply. In addition, a user must be specifically authorized to use a particular computing or network resource by the campus unit responsible for operating the resource.

Individual units within the University may define "conditions of use" for information technology resources under their control. These statements must be consistent with this overall Policy but may provide additional detail, guidelines and/or restrictions. **Such policies may not relax or subtract from, this policy.** Where such "conditions of use" exist, enforcement mechanisms defined

therein shall apply. These individual units are responsible for publicizing both the regulations they establish and their policies concerning the authorized and appropriate use of the equipment for which they are responsible. In such cases, the unit administrator shall provide the Vice President for Finance & Operations with a copy of such supplementary policies prior to implementation thereof. Where use of external networks is involved, policies governing such use also are applicable and must be adhered to.

3.0 Policy

3.1 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 Oklahoma State University 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 requires that members of its community act in accordance with these responsibilities, this Policy, the University's Student or Faculty Handbook, as appropriate, OSU Policies and Procedures, relevant laws and contractual obligations, and the highest standard of ethics. The policies as stated in this Policy are intended to ensure that users of University information resources shall:
 - i. respect software copyrights and licenses
 - ii. respect the integrity of computer-based information resources

- iii. refrain from seeking to gain unauthorized access
 - iv. respect the privacy of other computer users
- D. 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.
- E. 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.

3.2 Authorized User Purposes

- 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 except in connection with scholarly pursuits (such as faculty publishing activities) in accordance with the University consulting policy or the policy governing Access by External Entities to University Technology Resources, or in a purely incidental way. State law generally prohibits the use of University 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.

3.3 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. Liability for any loss or damage shall be limited to a credit for fees and charges paid to the University for use of the computing facilities which resulted in the loss or damage.
- C. 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.
- D. An individual using University computing resources or facilities must do so in the knowledge that he/she is using University resources in support of his/her work. The University owns everything stored in its facilities 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.
- E. Any individual using University computing resources and facilities must realize that all computer systems maintain internal audit trails 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.
 - F. 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 come 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.

3.4 Conduct Expectations and Prohibited Actions

- A. The well-being of all computer users 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 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 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. Computer users shall not use network links for any use other than permitted in network guidelines (e.g., ONENET, Internet, NSFNet, BITNET). 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. Some public bulletin boards may be designated for selling items, etc., and must be used appropriately, according to the stated purpose of the list(s). Vendors may send product information and technical material to specific mailing lists, with the permission of the manager of the mailing list.
- 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.

3.5 System Administrator Responsibilities

- A. The **Board of Regents** for Oklahoma State University and the Agricultural and Mechanical Colleges is 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 Oklahoma State University unless a written contract signed by the suitable contracting authority exists to the contrary. Day-to-day control of any particular system resides with the head of a specific subdivision of the University structure, such as a Division Head, Department Head, or Director.
- 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. In order to do so, functional guidelines regarding who is granted access to the various components of the University's computing information resources have been developed and will be updated from time to time through internal management guidelines developed by the IT, and approved by the OSU-OKC VP Council.
- C. The "Access Control List" 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 University official in charge of a particular unit or system may designate another person or persons to manage the system. This person (or persons), or the owner in the absence of such a designation, is the "system administrator". The system administrator's use of the University's computing resources is governed by the same guidelines that apply to any other user. However, the system administrator has additional responsibilities and authorities with respect to the system under his/her control and its users.
- E. The system administrator has certain responsibilities to the University as a whole for the system(s) under his/her control, regardless of the policies of his/her department or group, and the owner has the ultimate responsibility to see that these are carried out by the system administrator. These responsibilities are:

OSU-Oklahoma City Technology Polices

- 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.
 - iv. To promulgate information about specific policies and procedures that govern access to and use of the system and services provided to the users or explicitly not provided. This information should describe the data backup services, if any, offered to the users. A written document given to users or messages posted on the computer system itself shall be considered adequate notice.
 - v. To cooperate with the system administrators of other computer systems or networks, whether within or without Oklahoma State University, to find and correct problems caused on another system by the use of the system under his/her control.
- F. 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.
- G. 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.
- H. 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 permission to access the data from the Vice President for Finance & Operations or designee of such officer.
 - ii. An appropriate form with the signature of the Vice President for Finance & Operations shall be presented to the system administrator allowing the system administrator to proceed to access the data.
 - iii. The individual whose account has been accessed will be notified as soon as possible by copy of the above referenced form. Where necessary to ensure the integrity of an investigation into the use of University computing resources, such notice, with the approval of the Executive Vice President, may be delayed until such time as such investigation would no longer be compromised.
- I. System administrators are required to report suspected unlawful or improper activities to the proper University authorities. 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.
- J. 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. In such cases, and a system administrator is required to access the individual's data, steps (1) and (2) set forth above in Section 3.5 (H) shall be followed and the Office of Legal Counsel shall be contacted and informed of the matter.

4.0 Enforcement

4.1 Consequences of Misuse of Computing Privileges

- A. Users, when requested, 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. Notify the user's instructor, department or division chair, or supervisor of the investigation.
 - ii. Suspend or restrict the user's computing privileges during the investigation.
 - iii. 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.
 - iv. Refer the matter for possible disciplinary action to the appropriate University department, i.e., the Office of the Vice President for Student Services, Vice President for Academic Affairs, or Vice President for Finance and Operations.
- C. Individuals whose privileges to access University computing resources have been suspended may request that the Vice President for Finance & Operations, or his/her designee, review the suspension. The Vice President for Finance & Operations, or designee, in his/her discretion, may reinstate privileges, alter any restrictions that have been imposed, or refuse to interfere with the administrative action taken to that time. There is no right to a hearing or appearance regarding such issues and the decision made by the Vice President for Finance & Operations or designee is final.

Network Security

1.0 Purpose

The network of Oklahoma State University-Oklahoma City (OSU-OKC) exists to facilitate the research, education and outreach missions of the University. The network provides electronic capabilities that allow OSU-Oklahoma City faculty, staff, students or affiliates to access information, share data, collaborate, and communicate. Information Technology (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.

2.0 Scope

This policy is applicable to all individuals using University owned or controlled computer and computer communication facilities or equipment. It is applicable to

all University information resources whether individually controlled or shared, stand alone or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the University. In addition, a user must be specifically authorized to use a particular computing or network resource by the campus unit responsible for operating the resource.

Individual units within the University may define "conditions of use" for information resources under their control. These statements must be consistent with this overall Policy but may provide additional detail, guidelines and/or restrictions. **Such policies may not relax or subtract from, this policy.** Where such "conditions of use" exist, enforcement mechanisms defined therein shall apply. These individual units are responsible for securing appropriate authorization (Per 2-0501 Administrative Information Systems policy) and to furnish IT with a copy of the approved document. Units must also publicize both the regulations they establish and their policies concerning the authorized and appropriate use of the equipment for which they are responsible. In such cases, the unit administrator shall provide the Vice President for Finance & Operations with a copy of such supplementary policies prior to implementation thereof. Where use of external networks is involved, policies governing such use also are applicable and must be adhered to.

3.0 Policy

3.1 OSU-Oklahoma City Network Components

A. The network consists of the following:

- i. **Access-Layer Network Infrastructure** - network wiring and electronics (network switches and/or hubs) in OSU-Oklahoma City buildings that interconnect OSU-Oklahoma City's computers and other devices.
- ii. **Wireless Network Access "Air Space"** - radio spectrum used for wireless network access at OSU-Oklahoma City.
- iii. **Network Backbone and Building Switches** - top-level network switches/routers in each building and the core OSU network backbone that connect OSU-Oklahoma City building networks together and to off-campus networks.
- iv. **Wide Area Network Connections** - Wide Area Network (WAN) that connects distributed portions of the OSU-Oklahoma City 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 and is operated in cooperation with the Oklahoma Office of State Finance.
- vi. **Core Network Services** - services required for (Domain Name Service, DHCP, WINS, etc.)
 - vii. **OSU-Oklahoma City Network** – the infrastructure to provide data and communication services and resources
 - viii. **Subordinate Departmental Network** – an independent network whose development has been reviewed by IT and approved by the responsible Vice President and is subject to approval by the OSU Executive Systems Council. (Per 2-0501 Administrative Information Systems policy)
 - ix. **OSU Research Network (non administrative)** – an independent network that is logically and physically independent of the OSU Network whose development has been reviewed by IT due to the potential risk to the production environment.

3.2 General Provisions

- A. **OSU 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.
- B. **Subordinate Departmental Network** - A departmental network is considered an independent system and **shall not be directly interfaced with any institutional system (per 2-0501 Administrative Information Systems policy). Any deviation to this must be reviewed by IT and approved by the Vice President for Finance & Operations.**
- C. **Research Network (non administrative)**– Research that requires a less restrictive environment than the OSU Network may be connected to the OSU Research Network, as the current infrastructure allows. It is possible funding may be required for such a connection.
- D. **Wireless Network** - Wireless services are subject to the same rules and policies that govern other Information Technology at OSU (examples include: Appropriate Use Policy, Use of Electronic Mail, World Wide Web Publishing Policy). Wireless equipment and users must follow general wireless communication protocols. Wireless access will be provided for public access in some public areas, such as the Library. Communication links will not be encrypted and will be restricted to selective services. All

- other wireless access will be limited to authorized faculty, staff, students and affiliates. Users will be required to authenticate before any connection will be allowed. Logs of all access and authorizations should be kept for a period of ninety days. Standard wireless encryption is to be used on all devices as appropriate. Anti-Virus Software is to be used on all devices as appropriate. All wireless needs should be directed to IT for review and coordination.
- E. **Extension of the Backbone into New Buildings** - The extension of the network into new buildings on campus(s) and building renovations should be included and funded as part of building construction projects. Buildings should not be erected and renovations should not be done without the capability to communicate with the OSU network or without IT approval, blueprints, or IT involvement during construction. Installation of any communications wiring and/or facilities shall be performed in accordance to industry standards and requirements set forth by IT.
 - F. **TCP/IP – OSU-Oklahoma City'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 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., unless special arrangements are made with IT and approved by the Director IT. Departments maintaining their own networks must use other space for their equipment and cable. At no time shall any wiring not belonging to IT be located within a IT wiring closet without expressed written approval from IT.

- I. **Exceptions to Interim Network Policy Requirements and Guidelines** - Requests for an exception to a requirement or guideline of this policy should be directed to IT for coordination and approval.
- J. **Mediation** - If mediation is required, issues will be presented to an appropriate advisory committee for review. All decisions will be communicated in writing and will include justification for the decision.

3.3 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 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-Oklahoma City Network Connections to Other Networks** - IT maintains relationships and agreements with OneNet and other service providers to keep the OSU-Oklahoma City Network well connected to the commercial Internet and academic networks. IT administers all interfaces between networks and connections between the OSU-Oklahoma City Network and other networks.
- D. **Administration of OSU –OKC Network Name and Address Space** - IT manages the OSU network name space and the assignment of names and network addresses (IP numbers) for security and identity of users.
- E. **Administration of OSU Wireless Networking** - IT manages the radio spectrum for use of wireless networking at OSU-Oklahoma City to ensure compatible access to all OSU-Oklahoma City 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 Network causing

outages and reliability problems to all or part of the network. Devices not approved for use on OSU's Data Communication 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-Oklahoma City 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
- M. **Systems Security Officer (SSO)** –OSU-Oklahoma City's SSO or the person designated by the Director of IT, shall be the primary contact to work in conjunction with appropriate university officials for the interpretation, enforcement and monitoring of this policy and the resolution of problems concerning it. Any issues concerning law shall be referred to VP Council and OSU Stillwater's SSO advice and action as applicable. In situations that are an immediate threat to the security or operation of a computer or network, the SSO may require immediate intervention of access privileges and affected user files or messages. In such an emergency, the SSO will notify, as soon as possible, the appropriate university administrators and users affected by the situation.

3.4 Division or Department Responsibilities

- A. **Coordination of Computer and Network Security** - The Division Head or Director in each departmental major unit is the person in charge of delegating

the coordination of computer security in each area. He or she should identify a security liaison that has the following responsibilities for the division or unit:

- i. **The Security Liaison** - Works with IT staff to track down and correct excessive use of network resources, especially off-campus network usage. Encourages members of the unit to utilize network bandwidth and resources efficiently. Acts as a liaison between IT and network users for the purpose of scheduling maintenance periods, coordinating system changes, and disseminating information concerning the OSU network.
- ii. **Network Security Maintenance** - The security liaison implements and maintains sound network and computer security practices in the unit. This includes, but is not limited to, host-based security mechanisms such as password-protected logins, file protections, ensuring all machines run anti-virus software and security patch maintenance on all machines. System Administrators are also to encourage end-users to select secure passwords and change them regularly, and encouraged to use security-minded, IT authorized access tools.
- iii. **Network Name and Address Coordination** - The security liaison serves as the unit coordination point for the assignment of network name and addresses.

3.5 User Responsibilities

- A. The primary users of computers connected to the OSU-Oklahoma City network are responsible for the following:
 - i. **Abiding by OSU-Oklahoma City's Appropriate Technology Use Policy** - Users should efficiently use network resources and follow OSU-Oklahoma City'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 IT HelpDesk , and cooperate with support staff in correcting malfunctions.

- iii. **Taking Proper Security Precautions** - Users should select secure passwords and change them regularly. Security-minded network access techniques should be used whenever practical.
- iv. **Keeping the Operating System Secure** - Users should make sure their computer's operating system is kept up-to-date with current security patches. This may be accomplished by the owner, local support staff, or IT.
- 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-Oklahoma City's Network will be disabled to ensure the stability and availability of the network

4.0 Enforcement

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

Specific Policies (Technology Professionals)

Server Security

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by OSU-Oklahoma City. Effective implementation of this policy will minimize unauthorized access to OSU-Oklahoma City proprietary information and technology.

2.0 Scope

This policy applies to server equipment owned and/or operated by OSU-Oklahoma City, and to servers registered under any OSU-Oklahoma City-owned internal network domain.

This policy is specifically for equipment on the internal OSU-Oklahoma City network. For secure configuration of equipment external to OSU-Oklahoma City on the DMZ, refer to the *DMZ Lab Security Policy*.

3.0 Policy

3.1 Ownership and Responsibilities

- A. All internal servers deployed at OSU-Oklahoma City 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 with IT. 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 IT must be kept up-to-date.
- D. Configuration changes for production servers must follow the appropriate change management procedures.

3.2 General Configuration Guidelines

- A. Operating System configuration should be in accordance with approved IT guidelines.
- 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.
- 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.

3.3 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.

3.4 Compliance

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

4.0 Enforcement

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

5.0 Definitions

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

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

6.0 Revision History

Internal Lab Security

1.0 Purpose

This policy establishes information security requirements for OSU-Oklahoma City labs to ensure that OSU-Oklahoma City confidential information and technologies are not compromised, and that production services and other OSU-Oklahoma City interests are protected from lab activities.

2.0 Scope

This policy applies to all internally connected labs, OSU-Oklahoma City employees and third parties who access OSU-Oklahoma City's labs. All existing and future equipment, which fall under the scope of this policy, must be configured according to the referenced documents. DMZ Labs and stand-alone, air-gapped labs are exempt from this policy. DMZ labs must comply with the *DMZ Lab Security Policy*.

3.0 Policy

3.1 Ownership Responsibilities

- A. Lab owning organizations are responsible for assigning lab managers, a point of contact (POC), and a back-up POC for each lab. Lab owners must maintain up-to-date POC information with IT. Lab managers or their backup must be available around-the-clock for emergencies, otherwise actions will be taken without their involvement.
- B. Lab managers are responsible for the security of their labs and the lab's impact on the university production network and any other networks. Lab managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined lab managers must do their best to safeguard OSU-Oklahoma City from security vulnerabilities.
- C. Lab managers are responsible for the lab's compliance with all OSU-Oklahoma City security policies. The following are particularly important: *Password Policy for networking devices and hosts, Wireless Security Policy, Anti-Virus Policy, and physical security*.
- D. The Lab Manager is responsible for controlling lab access. Access to any given lab will only be granted by the lab manager or designee, to those individuals with an immediate business need within the lab, either short-term or as defined by their ongoing job function. This includes continually

- monitoring the access list to ensure that those who no longer require access to the lab have their access terminated.
- E. IT must maintain a firewall device between the university production network and all lab equipment.
 - F. IT reserves the right to interrupt lab connections that impact the university production network negatively or pose a security risk.
 - G. The Network Support Organization must record all lab IP addresses, which are routed within OSU-Oklahoma City networks, in Enterprise Address Management database along with current contact information for that lab.
 - H. Any lab that wants to add an external connection must provide a diagram and documentation to IT with business justification, the equipment, and the IP address space information. IT will review for security concerns and must approve before such connections are implemented.
 - I. All user passwords must comply with OSU-Oklahoma City's *Password Policy*. In addition, individual user accounts on any lab device must be deleted when no longer authorized within three (3) days. Group account passwords on lab computers (Unix, windows, etc) must be changed every semester. For any lab device that contains OSU-Oklahoma City proprietary information, group account passwords must be changed within three (3) days following a change in group membership.
 - J. No lab shall provide production services. Production services are defined as ongoing and shared business critical services that generate revenue streams or provide customer capabilities. These should be managed by a IT.
 - K. IT will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

3.2 General Configuration Requirements

- A. All traffic between the university production and the lab network must go through a IT maintained firewall. Lab network devices (including wireless) must not cross-connect the lab and production networks.
- B. Original firewall configurations and any changes thereto must be reviewed and approved by IT.

- C. IT may require security improvements as needed.
- D. Labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the production network and/or non-OSU-Oklahoma City networks. These activities must be restricted within the lab.
- E. Traffic between production networks and lab networks, as well as traffic between separate lab networks, is permitted based on business needs and as long as the traffic does not negatively impact on other networks. Labs must not advertise network services that may compromise production network services or put lab confidential information at risk.
- F. IT reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals.
- G. Lab owned gateway devices are required to comply with all OSU-Oklahoma City product security advisories and must authenticate against the University Authentication servers.
- H. The enable password for all lab owned gateway devices must be different from all other equipment passwords in the lab. The password must be in accordance with OSU-Oklahoma City's *Password Policy*. The password will only be provided to those who are authorized to administer the lab network.
- I. In labs where non-OSU-Oklahoma City personnel have physical access (e.g., training labs), direct connectivity to the production network is not allowed. Additionally, no OSU-Oklahoma City confidential information can reside on any computer equipment in these labs. Connectivity for authorized personnel from these labs can be allowed to the production network only if authenticated against the Authentication servers, temporary access lists (lock and key), SSH, client VPNs, or similar technology approved by IT.
- J. Infrastructure devices (e.g. IP Phones) needing university production network connectivity must adhere to the *Network Security Policy*.
- K. All lab external connection requests must be reviewed and approved by IT. Analog or ISDN lines must be configured to only accept trusted call numbers. Strong passwords must be used for authentication.

- L. All labs networks with external connections must not be connected to OSU-Oklahoma City university production network or any other internal network directly or via a wireless connection, or via any other form of computing equipment. A waiver from IT is required where air-gapping is not possible (e.g., Partner Connections to third party networks).

4.0 Enforcement

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

5.0 Definitions

Term	Definition
Internal Lab	A lab that is within OSU-Oklahoma City's firewall and connected to the university production network
Lab Manager	The individual responsible for all lab activities and personnel
Lab	A Lab is any non-production environment, intended specifically for developing, demonstrating, training and/or testing of a product.
External Connections (also known as DMZ)	External connections include (but not limited to) third-party data network-to-network, analog and ISDN data lines, or any other Telco data lines.
Lab Owned Gateway Device	A lab owned gateway device is the lab device that connects the lab network to the rest of OSU-Oklahoma City network. All traffic between the lab and the production network must pass through the lab owned gateway device unless approved by IT.
Telco	A Telco is the equivalent to a service provider. Telcos offer network connectivity, e.g., T1, T3, OC3, OC12 or DSL. Telcos are sometimes referred to as "baby bells", although Sprint and AT&T are also considered Telcos. Telco interfaces include BRI, or Basic Rate Interface - a structure commonly used for ISDN service, and PRI, Primary Rate Interface - a structure for voice/dial-up service.
Traffic	Mass volume of unauthorized and/or unsolicited network Spamming/Flooding traffic.
Firewall	A device that controls access between networks. It

	can be a PIX, a router with access control lists or similar security devices approved by IT.
Extranet	Connections between third parties that require access to connections non-public OSU-Oklahoma City resources, as defined in IT's Extranet policy (link).
DMZ (De-Militarized Zone)	This describes network that exists outside of primary firewalls, but are still under OSU-Oklahoma City administrative control.

6.0 Revision History

De-Militarized Zone Lab Security

1.0 Purpose

This policy establishes information security requirements for all networks and equipment deployed in OSU-Oklahoma City labs located on the "De-Militarized Zone" (DMZ). Adherence to these requirements will minimize the potential risk to OSU-Oklahoma City from the damage to public image caused by unauthorized use of OSU-Oklahoma City resources, and the loss of sensitive/company confidential data and intellectual property.

2.0 Scope

OSU-Oklahoma City Lab networks and devices (including but not limited to routers, switches, hosts, etc.) that are Internet facing and located outside OSU-Oklahoma City Internet firewalls are considered part of the DMZ Labs and are subject to this policy. This includes DMZ Labs in primary Internet Service Provider (ISP) locations and remote locations. All existing and future equipment, which falls under the scope of this policy, must be configured according to the referenced documents. This policy does not apply to labs residing inside OSU-Oklahoma City's Internet firewalls. Standards for these labs are defined in the *Internal Lab Security Policy*

3.0 Policy

3.1. Ownership and Responsibilities

- A. All new DMZ Labs must present a business justification with sign-off at the business unit Vice President level. IT must keep the business justifications on file.

- B. Lab owning organizations are responsible for assigning lab managers, point of contact (POC), and back up POC, for each lab. The lab owners must maintain up to date POC information with IT. Lab managers or their backup must be available around-the-clock for emergencies.
- C. Changes to the connectivity and/or purpose of existing DMZ Labs and establishment of new DMZ Labs must be requested through IT, for a thorough technical, and safety review, and approved by VP Council.
- D. All ISP connections must be maintained by IT
- E. IT must maintain a firewall device between the DMZ Lab(s) and the Internet.
- F. IT reserve the right to interrupt lab connections if a security concern exists.
- G. The DMZ Lab will provide and maintain network devices deployed in the DMZ Lab up to IT point of demarcation.
- H. IT must record all DMZ Lab address spaces and current contact information.
- I. The DMZ Lab Managers are ultimately responsible for their DMZ Labs complying with this policy.
- J. Immediate access to equipment and system logs must be granted to members of IT upon request, in accordance with the *Audit Policy*
- K. Individual lab accounts must be deleted, or disabled within three (3) days when access is no longer authorized.
- L. Group account passwords must comply with the *Password Policy* and must be changed within three (3) days from a change in the group membership.
- M. IT will address non-compliance waiver requests on a case-by-case basis.

3.2. General Configuration Requirements

- A. Production resources must not depend upon resources on the DMZ Lab networks.

- B. DMZ Labs must not be connected to OSU-Oklahoma City's production networks, either directly or via a wireless connection.
- C. DMZ Labs should be in a physically separate room from any internal networks. If this is not possible, the equipment must be in a locked rack with limited access. In addition, the Lab Manager must maintain a list of who has access to the equipment.
- D. Lab Managers are responsible for complying with the following related policies:
 - i. *Password Policy*
 - ii. *Network Security Policy*
 - iii. *Appropriate Technology Use Policy*
- E. The Network Support Organization maintained firewall devices must be configured in accordance with least-access principles and the DMZ Lab business needs. All firewall filters will be maintained by IT.
- F. The firewall device must be the only access point between the DMZ Lab and the rest of OSU-Oklahoma City's networks and/or the Internet. Any form of cross-connection which bypasses the firewall device is strictly prohibited.
- G. Original firewall configurations and any changes thereto must be reviewed and approved by IT (including both general configurations and rule sets). IT may require additional security measures as needed.
- H. Traffic from DMZ Labs to the OSU-Oklahoma City internal network, including VPN access, falls under the *Remote Access Policy*
- I. All routers and switches not used for testing and/or training must conform to the DMZ Router and Switch standardization documents.
- J. Operating systems of all hosts internal to the DMZ Lab running Internet Services must be configured to the secure host installation and configuration standards.
- K. Current applicable security patches/hot-fixes for any applications that are Internet services must be applied. Administrative owner groups must have processes in place too stay current on appropriate patches/hotfixes.
- L. All applicable security patches/hot-fixes recommended by the vendor must be installed.

- M. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
- N. Services and applications not serving business requirements must be disabled.
- O. OSU-Oklahoma City Confidential information is prohibited on equipment in labs where non-
- P. OSU-Oklahoma City personnel have physical access (e.g., training labs), in accordance with the *OSU policies*.
- Q. Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.

4.0 Enforcement

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

5.0 Definitions

Terms	Definitions
Access Control List (ACL)	Lists kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).
DMZ (de-militarized zone)	Networking that exists outside of OSU-Oklahoma City primary firewalls, but is still under OSU-Oklahoma City administrative control.
Least Access Principle	Access to services, hosts, and networks is restricted unless otherwise permitted.
Internet Services	Services running on devices that are reachable from other devices across a network. Major Internet services include DNS, FTP, HTTP, etc.
IT Point of Demarcation	The point at which the networking responsibility transfers from IT to the DMZ Lab. Usually a router or firewall.
Lab Manager	The individual responsible for all lab activities and personnel.
Lab	A Lab is any non-production environment, intended specifically for developing,

	demonstrating, training and/or testing of a product.
Firewall	A device that controls access between networks., such as a PIX, a router with access control lists, or a similar security device approved by IT.
Internally Connected Lab	A lab within OSU-Oklahoma City's firewall and connected to the production network.

6.0 Revision History

Passwords on Accounts and Network Devices

1.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of OSU-Oklahoma City's entire university network. As such, all OSU-Oklahoma City student, faculty, and staff (including contractors and vendors with access to OSU-Oklahoma City systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any OSU-Oklahoma City facility, has access to the OSU-Oklahoma City network, or stores any non-public OSU-Oklahoma City information.

3.0 Policy

3.1 General

- 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.

3.2 Guidelines

- A. **General Password Construction Guidelines** - Passwords are used for various purposes at OSU-Oklahoma City. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords. Poor, weak passwords have the following characteristics:
 - i. The password contains less than eight characters
 - ii. The password is a word found in a dictionary (English or foreign)
 - iii. The password is a common usage word such as:
 - iv. Names of family, pets, friends, co-workers, fantasy characters, etc.
 - v. Computer terms and names, commands, sites, companies, hardware, software.
 - vi. The words "OSU-Oklahoma City", "sanjose", "sanfran" or any derivation.
 - vii. Birthdays and other personal information such as addresses and phone numbers.

- viii. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- ix. Any of the above spelled backwards.
- x. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- xi. Strong passwords have the following characteristics:
- xii. Contain both upper and lower case characters (e.g., a-z, A-Z)
- xiii. Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&*()_+|~-=\`{}[]:;'<>?,./)
- xiv. Are at least five alphanumeric characters long.
- xv. Are not a word in any language, slang, dialect, jargon, etc.
- xvi. Are not based on personal information, names of family, etc.
- xvii. Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
- xviii. Do not use either of these examples as passwords!

B. Password Protection Standards - Do not use the same password for OSU-Oklahoma City accounts as for other non-OSU-Oklahoma City access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various OSU-Oklahoma City access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share OSU-Oklahoma City passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential OSU-Oklahoma City information.

Here is a list of "dont's":

- i. Don't reveal a password over the phone to ANYONE
- ii. Don't reveal a password in an email message
- iii. Don't reveal a password to the boss
- iv. Don't talk about a password in front of others
- v. Don't hint at the format of a password (e.g., "my family name")
- vi. Don't reveal a password on questionnaires or security forms
- vii. Don't share a password with family members
- viii. Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in IT.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger). Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to IT and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by IT or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- i. should support authentication of individual users, not groups.
- ii. should not store passwords in clear text or in any easily reversible form.
- iii. should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- iv. should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

4.0 Enforcement

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

5.0 Definitions

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

6.0 Revision History

Remote Access

1.0 Purpose

The purpose of this policy is to define standards for connecting to OSU-Oklahoma City's network from any host. These standards are designed to minimize the potential exposure to OSU-Oklahoma City from damages which may result from unauthorized use of OSU-Oklahoma City resources. Damages include the loss of sensitive or university confidential data, intellectual property, damage to public image, damage to critical OSU-Oklahoma City internal systems, etc.

2.0 Scope

This policy applies to all OSU-Oklahoma City employees, contractors, vendors and agents with a OSU-Oklahoma City-owned or personally-owned computer or workstation used to connect to the OSU-Oklahoma City network. This policy applies to remote access connections used to do work on behalf of OSU-Oklahoma City, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

- A. It is the responsibility of OSU-Oklahoma City employees, contractors, vendors and agents with remote access privileges to OSU-Oklahoma City's production network to ensure that their remote access connection is given the same consideration as the user's on-site connection to OSU-Oklahoma City.
- B. General access to the Internet for recreational use by immediate household members through the OSU-Oklahoma City Network on personal computers is permitted for employees that have flat-rate services. The OSU-Oklahoma City employee is responsible to ensure the family member

does not violate any OSU-Oklahoma City policies, does not perform illegal activities, and does not use the access for outside business interests. The OSU-Oklahoma City employee bears responsibility for the consequences should the access be misused.

- C. Please review the following policies for details of protecting information when accessing the production network via remote access methods, and acceptable use of OSU-Oklahoma City's network:
 - i. Wireless Communications Policy
 - ii. Acceptable Technology Policy
- D. For additional information regarding OSU-Oklahoma City's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

3.2 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-Oklahoma City employee provide their login or email password to anyone, not even family members.
- C. OSU-Oklahoma City employees and contractors with remote access privileges must ensure that their OSU-Oklahoma City-owned or personal computer or workstation, which is remotely connected to OSU-Oklahoma City's production 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-Oklahoma City employees and contractors with remote access privileges to OSU-Oklahoma City's production network must not use non-OSU-Oklahoma City email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct OSU-Oklahoma City business, thereby ensuring that official business is never confused with personal business.
- E. Routers for dedicated ISDN lines configured for access to the OSU-Oklahoma City 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-Oklahoma City 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-Oklahoma City's networks must meet the requirements of OSU-Oklahoma City-owned equipment for remote access.
- K. Organizations or individuals who wish to implement non-standard Remote Access solutions to the OSU-Oklahoma City production network must obtain prior approval from IT.

4.0 Enforcement

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

5.0 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. Cable Modems are becoming increasingly popular.
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.

Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Production network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a OSU-Oklahoma City-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into OSU-Oklahoma City and an ISP, depending on packet destination.
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).
Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.
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-Oklahoma City's production network through a non-OSU-Oklahoma City controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-OSU-Oklahoma City network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into OSU-Oklahoma City's production network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

6.0 Revision History

Audit

1.0 Purpose

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

Audits may be conducted to:

- i. Ensure integrity, confidentiality and availability of information and resources
- ii. Investigate possible security incidents ensure conformance to OSU-Oklahoma City security policies
- iii. Monitor user or system activity where appropriate.

2.0 Scope

This policy covers all computer and communication devices owned or operated by OSU-Oklahoma City. This policy also covers any computer and communications device that are present on OSU-Oklahoma City premises, but which may not be owned or operated by OSU-Oklahoma City.

3.0 Policy

When requested, and for the purpose of performing an audit, any access needed will be provided to members of IT.

This access may include:

- i. User level and/or system level access to any computing or communications device
- ii. Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on OSU-Oklahoma City equipment or premises
- iii. Access to work areas (labs, offices, cubicles, storage areas, etc.)
- iv. Access to interactively monitor and log traffic on OSU-Oklahoma City networks

4.0 Enforcement

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

5.0 Definitions

6.0 Revision History