Section 6: User Accounts and Acceptable Use

Telecommunication resources of the University are provided for the use of students, faculty, and staff to help carry out the mission of the University. The University encourages and promotes uses of telecommunication resources by the University community that support this mission.

Telecommunication systems include all voice, data, and video hardware and software owned by the University as well as any communications hardware and software provided by the University for the purpose of accessing its access points or any computer network governed in part or whole by the University.

The University's Telecommunications Network is composed of four major areas:

1. Voice – campus telephones and services
2. Wireless – smartphones and push-to-talk services
3. Data – IP data services wired and wireless
4. Video – conference rooms and web collaboration

Voice

General Description

Use of the voices services are provided to the University community are subject to all applicable University, State, and Federal usage guidelines. Violation of these guidelines may result in loss of usage privileges and/or disciplinary action. Repair and/or installation are the responsibility of Information Systems.

Telephone Usage Policies

Individual groups or projects within NSU may adopt more restrictive telephone (voice network) usage policies that may apply to the personnel within their area.

Acceptable Uses

Acceptable uses are as follows:

- Conduct of University business
- Recruitment or enrollment drive efforts

- Communication for professional development
- Other administrative communications or activities in direct support of the University

Prohibited Uses

Prohibited Uses are as follows:

- Any non-University business
- Political campaigns
- The use of the University telephone system by a University employee for the solicitation of non-University goods or service
- Monitoring or recording of telephone conversations with or without the knowledge of the on-line parties

Procedure to Request Analog Telephone Service

The procedure to request analog telephone service is as follows:

- Submit a service request to http://support.nsula.edu
- Provide a clear justification for telephone service in the service request
- If facilities are available, the request can be approved and telephone service installed
- Equipment purchases, including the cost of associated network equipment and wiring, are the responsibility of the requesting budget unit.

Procedure to Request Digital Telephone Service

The procedure to request digital telephone service is as follows:

- Submit a service request to http://support.nsula.edu
- Provide a clear justification from the Department Head requesting that a digital telephone be provided to a faculty or staff member. *(Due to the high cost digital phones only will be granted in a validated application. Graduate Assistant and Student Workers will not be eligible for a digital phone.)*
- If facilities are available, the request can be approved and telephone service installed
- Digital telephone purchases, including the cost of associated network equipment and wiring, are the responsibility of the requesting budget unit.

Procedure to Request LINC Access

The procedure to request LINC access is as follows:

- Submit a service request to http://support.nsula.edu
- Provide a clear justification from the Department Head requesting that LINC access is given to a faculty or staff member.

- With the activation of LINC access, a monthly LINC report will be generated and forwarded to each Department having personnel with LINC access. The report must be signed by the user and returned to Information Systems by the date indicated on the attached memorandum.
- Failure to return a LINC report by the date indicated on the memorandum will result in the deactivation of LINC access. Reports may be faxed to Information Systems at 357-5745.
- LINC access will also be deactivated for anyone that is terminated or resigns. This information is provided to Information Systems from Human Resources.

Procedure to Request International Calling Access

The procedure to request an International Calling is as follows:

- Submit a service request to http://support.nsula.edu
- Provide a clear justification from the Department Head requesting that an International Calling Card be provided to a faculty or staff member.
- If the request is approved, service to the extension requesting service

Wireless Service

General Description

Cellular wireless services are available to University faculty, staff, and administrative personnel. A wide range of coverage and options are available from which to choose. Contract Information Systems for complete details and pricing.

Procedure to Request a Cell Phone

The procedure to request a cell phone is as follows:

- Submit a service request to http://support.nsula.edu
- Provide a clear justification from the Department Head (*Student workers, Graduate Assistants, and non-University personnel are not eligible for cell phone service)*
- The CIO or Deputy CIO will forward the request to the requesting agents vice president for approval
- The CIO or Deputy CIO will forward approvals to Business Affairs to verify funding
- Upon approval by the reporting vice president and Business Affairs, Information Systems staff will process the order for service
- Information Systems will notify the requestor when the device is received and ready for pickup.

Data

General Description

The University Network is defined to include any and all computer-based communications facilities, which are owned or operated under the supervision of the University. The University Network is for use by authorized persons legitimately affiliated with NSU, consistent with, and in the course of, their official work, study, and/or research. The Network Administrator manages the University network.

The following restrictions apply to the Northwestern network:

- The Network Administrator must approve all physical connections/modifications to the university network.
- The Network Administrator must approve any network hardware and software, before purchase. Any purchase requisition related to network hardware or software must have the approval of the Network Administrator before the purchase can be made.
- Information Systems must approve any data wiring being installed. Information Systems will oversee all contract data wiring purchased by the University. Payment for such work will not be rendered until Information Systems approves all work performed.
- Any network wiring will be conducted by one of the contractors approved by OTM on the state contract. These contractors will work under the supervision of Information Systems.
- The cost of all data wiring will be the responsibility of the associated budget unit or grant.
- No wireless network access points or other such related hardware may be purchased or installed without the approval of the Network Administrator. Wireless technologies present network security issues if not implemented properly. The Network Administrator will approve and supervise any such installation or purchase.

Network Usage Policies

Individual groups or projects within NSU may adopt more restrictive network usage policies that apply to their sub-networks and personnel within their area.

Acceptable Uses

Acceptable uses are as follows:

- Communication for professional development, to maintain current information pertaining to university business or academics, or to collaborate in research and education
- As a means for authorized users to have legitimate access to remote facilities
- The publication of information via the Internet's World Wide Web (WWW), File Transfer Protocol (FTP), or similar techniques
- Other administrative communications or activities in direct support of NSU projects and missions

Prohibited Uses include

Prohibited uses are as follows:

- Use for personal or for-profit activities.
- Use by friends, family members, relatives, or others not officially affiliated with and authorized by the University. The University networks, including wireless, are not available as a substitute for private Internet service providers.
- Any use that is likely, or intended, to cause unauthorized network disruption, system failure, or information loss.
- Any use related to achieving, enabling, or hiding unauthorized access to systems, software, or information either within or outside NSU.
- Direct dial-up to a computer or network device connected to the university network
- Hosting any type of server on a personal computer
- Running any application that consumes an excessive amount of bandwidth. The CIO or Deputy CIO, on the advice of the Network Administrator and/or the System Administrator shall be the sole judge in determining "excessive bandwidth"
- Any unauthorized or illegal downloading or transfer of copyrighted material.
- Any use which violates Northwestern EDP administrative policies.
- Operating a wireless access point or wireless network on campus.

Internet Use Policy

The University subscribes to its Internet Service Provider's Use Policy as follows:

The use of University network facilities, including the NSU network for Internet access, for any reason other than for University related activities, is strictly forbidden. Violators may lose access to University facilities and/or the University network and be subject to state or federal civil or criminal penalties.

LONI Network Acceptable Use Policy

Network access facilitates the LONI participants in meeting their business needs. LONI reserves the right to monitor all network communications. With the exception of information protected by federal/state statutes and agency policies, users should have no expectation of privacy as to their network usage.

Participants may not download, store, transmit, or display any kind of image or document that violates federal, state, or local laws and regulations, executive orders, or that violates any state or department adopted policies, procedures, standards, or guidelines.

Acceptable use must be legal, ethical, and respectful of intellectual property, ownership of data, systems security mechanisms, and individual rights to privacy and freedom from intimidation, harassment and annoyance. An abuse of the privilege of the network use may result in disciplinary action as deemed appropriate by supervising authorities.

The LONI Network can be used for any legal purpose, so long as it does not interfere with or adversely affect the operation of the LONI Network or any participant, as may be determined by LONI.

LONI and its participants agree to take reasonable steps, individually and collectively, to ensure use of the LONI Network by participants and any other user is consistent with the terms of LONI's AUP.

The participants agree not to intentionally violate or tamper with the operation, performance or security of the LONI Network. Participants also agree to operate equipment that is attached to the LONI Network Service in a manner that does not adversely impact the performance of the LONI Network or other participant's equipment.

Internet Server Policies

University web sites (hosted under the nsula.edu domain) will adhere to the following policies:

- Accounts are created on university servers for the publishing of information related to departments, colleges, and organizations. No personal web pages will be included on these pages despite the connection between the organization and the staff. If a personal account is discovered, the site will be removed without warning to the publisher. Personal accounts for faculty and staff are hosted on http://users.nsula.edu. Faculty and staff desiring web accounts must contact the University Webmaster to establish an account. All accounts are subject to review for appropriateness to the mission of the university, the accuracy and legality of the published data, and consistency with all applicable laws and policies.

- Each organization with a web presence will have a dedicated NSU faculty/staff member serve as a point of contact for the website. Those members may solicit external help in the creation of their web site provided they inform the Webmaster as to who is performing changes to the site.

- The University Webmaster reserves the right to remove any material found to be using unapproved elements. Access to the server will be removed if such elements are found to exist. For any questions, please contact the Webmaster.

Web Domains

Domain names have established standard. Below are examples on how domain names are to be formatted in relation to the organization it will represent:

- business.nsula.edu
- nursing.nsula.edu
- education.nsula.edu
- scholars.nsula.edu
- sacs.nsula.edu

University Web Pages

Changes to the NSU home page and secondary web pages will be made by Information Systems and will be coordinated with the approval of the vice president of technology

Changes to content pages will be made by the web page owner (e.g., colleges and departments). These pages will conform to future guidelines to be approved by the University. Information Systems may provide assistance according to available resources.

User Accounts

To use the NSU computer resources, a user must first be assigned a computer account. Students are eligible for an account if they are currently enrolled at NSU. All University employees are eligible for computer accounts.

All accounts will be unique and used by only one individual. The use of shared or group accounts is prohibited.

Student User Accounts

Student accounts are created and are assigned one of the following roles:

- Applicant – a person that has applied to attend the University
- Student – a person that is enrolled at the University
- Alumni – a person that has graduated or has attended the University

Below is a service chart for services that student accounts will receive based on role.

Service	Applicant	Student	Alumni
Portal	X	X	X
Office 365		X	Email only
Office Pro Advantage		X	
Labs		X	
Wireless		X	

If a user account has been assigned to a student and the student withdraws from the University, that account will be disabled.

Employee User Accounts

Employee accounts provide access to network and computer system resources. These accounts must be properly managed in accordance with applicable laws and university policy. The following subparagraphs delineate actions necessary to support account management.

Section X.19 of the Policy and Procedures Manual (PPM), Employee Separation and Exit Interview Procedures is the basic university policy that requires departments to notify Human Resources and Information Systems of personnel actions. In some cases, the Electronic Data Systems Policies and Standards may supplement the Policy and Procedure manual but it is not intended to override or replace the PPM.

User accounts for academic and staff personnel will be terminated when the employee no longer has an active assignment within the University community.

Reporting Changes in Employment Status

In accordance with Section X.19 of the Policy and Procedures Manual (PPM), Employee Separation and Exit Interview Procedures, identifying personnel changes that may require changes to administrative, faculty, and staff user accounts is the responsibility of the department/unit to which the employee is assigned.

Department Heads/Budget Unit Heads are responsible for notifying Human Resources and Information Systems in writing when an employee terminates employment, takes extended leave, moves to another job assignment outside the department/unit, or assumes a different position within the same department/unit that results in a change in the need to access systems/data. The written notification should be provided immediately following approval of the personnel action and include the following information:

- Employee Name
- Employee SSN or CWID
- Computer Username
- Effective Date
- Type of Action (e.g., Retirement, Resignation, Termination, Administrative Leave, and Transfer)
- Current Department
- New Department (if transfer)
- Additional information as appropriate

To provide a failsafe mechanism for identifying terminated employees and employees changing departments, Human Resources will also notify Information Systems when an employee terminates employment, takes extended leave, or moves to another job assignment outside the department/unit. This failsafe mechanism is deemed appropriate given the legal requirements for access to state resources (e.g., networks and computer systems) and the possible adverse consequences resulting from inappropriate access by a disgruntled former employee. This failsafe mechanism is not intended to eliminate responsibility for reporting personnel changes by department/unit heads.

Terminations for cause to include administrative leave will be brought to the attention of Information Systems by the most expeditious means possible. If notification is made other than in writing this does not replace the requirement for the normal written notification.

Termination of Employment

When an employee's association with the university ends (to include an employee being placed on administrative leave), all access by these employees will be disabled by Information Systems.

Department Transfer

When an employee is transferred to another department all access will be terminated by Information Systems with the exception of basic services. Employees must apply/reapply for access to administrative software modules and other systems/data when reassigned to another department/unit. Approval of such requests by the appropriate System Manager will be based on the assigned duties and responsibilities for the new position. The new permissions assigned to an employee will not take effect before the first day of employment in the new position.

Other Types of Transfers/Personnel Actions

Department/Budget Unit Heads must notify Information Systems in writing of any other types of transfers or personnel actions that may result in changes to access.

Extended Leave

Extended leaved is defined as an absence of two weeks or longer.

All accounts for personnel on extended leave will be disabled for the duration of the extended leave period. Following return from extended leave, Department/Budget Unit Heads must notify Information Systems in writing that the employee has returned from extended leave and that the access privileges of the employee need to be restored.

Eligibility for a User Account

To be eligible for a user account, the requester must meet one of the following qualifications:

- Be enrolled in courses as a student at Northwestern
- Be currently employed as a faculty member at Northwestern
- Be currently employed as a staff member at Northwestern
- Be currently employed as an administrator at Northwestern.
- Any exception to the above will require the written permission of the vice president of technology or provost.

Establishing a User Account

To establish a user account:

- Complete the Request for User Account form
- Submit the completed form to Information Systems
- A system administrator will verify that the requester is eligible for an account

- A system administrator or designee will create the account and set the initial password for the account
- The user will be provided with their username and initial password

Student accounts are created automatically based on data collected in Banner.

Adjunct Accounts

User accounts for adjuncts will be created upon receipt of the following:

- A contract signed by the Vice President of Academic Affairs and Provost.
- A properly completed and signed Request for User Account Form. However, if the adjunct has submitted a properly completed and signed Request for User Account Form within the past two years, the account will be enabled with only the signed contract as indicated above.

User accounts for adjuncts will be created with an effective start date of 30 days before the contract start date and with a termination date of 30 days after the contract end date. This will allow adjuncts time for pre- and post-class activities. Should an adjunct require more than 30 days at the end of a class (e.g., to work with a student with a grade of "I" or "IP"), then the adjunct may request the Vice President of Academic Affairs and Provost to extend the 30-day period to a maximum of 60 days.

Generic User Accounts

Although the sharing of usernames/passwords is specifically precluded by other sections of this policy, there may be special circumstances where shared usernames/passwords are desirable. Each situation where there may be a need for a generic account will be evaluated on a case-by-case basis. Such exceptions may be approved by the CIO or Deputy CIO when deemed appropriate, security is manageable, and the following considerations have been included in the evaluation for creating a generic account. The evaluation process will begin with the submission of a request to Information Systems.

- Generic accounts be used only for special situations (e.g., testing of potential students, access to labs by continuing education students) when the users do not otherwise qualify for a Northwestern account.
- Generic accounts shall only be enabled during those periods when specifically required (e.g., Freshman Connection or a lab session).
- Generic accounts will be restricted to certain physical locations as indicated by the requester.
- The user has requested a generic account with a shared username/password to include a justification for such an account and the location where the account is to be used.
- The CIO or Deputy CIO has, after consultation with appropriate Information Systems staff, determined the use of an account with a shared username/password will not introduce a security risk given its intended use when proper technical controls and procedures are implemented and followed.

Student Worker Access to Faculty and Staff PCs and Departmental Data

Department Heads may request student workers be able to logon to PCs within their departments and access departmental data residing on shared directories. To request student access to departmental PCs and data, the department must submit a service request to Information Systems http://support.nsula.edu with the following information:

- Student name and student account (username) information.
- Justification for providing student access to PCs and data.
- Beginning and end dates for which access is to be granted (access will not be granted for periods in excess of one year). All student access to faculty and staff PCs will be terminated effective the day after the last day of each Spring semester. A new request must be submitted to Information Systems for student access during the Summer term and subsequent semesters.
- The departmental shared directories that the student will need to access. The requester assumes all responsibility in regard to student access to this data.

It will be the responsibility of the department head to educate students of the following policy:

Student workers hereby agree to abide by the following rules in regard to being granted access to faculty and staff PCs.

- I will keep personal usernames/passwords confidential – usernames/passwords will not be shared with anyone and I will not use the username/password of another individual.
- Passwords will not be written or stored in plain text format.
- I will log off or lock the PC when leaving the immediate area unless the screen lock has been activated.
- I will not allow anyone to use a PC that has been signed on under another individual's username and password.
- I will not make or permit unauthorized use of any information in the computer or hard copy files.
- I will not seek personal benefit or permit others to benefit personally by any confidential information that has come to them through their work assignment(s).
- I will not display or divulge the contents of any record or report in any manner to any person except in the conduct of their regular work assignment(s).
- I will not include knowingly or cause to be included in any record or report a false, inaccurate, or misleading entry.
- I will ensure that all printed output containing personal information is shredded.
- I will not allow photographs to be made of any display device (e.g., computer monitor) containing personal information.

- I will ensure that computer monitors are positioned in such a manner that unauthorized personnel cannot read personal or sensitive information.
- I will not aid, abet, or act in conspiracy with any other person to violate any part of the above.

User Name Scheme

All users will be assigned a unique username. The following naming scheme will be followed in the assignment of computer usernames:

Faculty/Staff/Administrative Usernames

Faculty/Staff/Administrative usernames will be automatically created using the following convention:

Last name
Plus 1st character of first name

If already in use, the first two characters of the first name will be used. See the following examples for how further duplicates will be handled:

Example: JOHN W. SMITH
1st - SMITHJ
2nd - SMITHJO
3rd - SMITHJOH
4th - SMITHJOHN
5th – SMITHJOHNW

Student Usernames

Student usernames will be automatically created using the following convention:

first initial + up to 13 characters of last name + last 6 digits of CWID

Example: vdemon456789 - Victor Demon with CWID 123456789

Usernames for students are intended to be permanent.

Password Assignments

An initial password will be assigned with every username. This initial password must be changed by the user by visiting the university portal at http://my.nsula.edu.

Faculty/Staff Password Assignments

If a faculty or staff member loses or forgets their password, they first should use the password reset feature with the university portal at http://my.nsula.edu/. If the user's security profile has never been setup, they must contact Information Systems (318-357-5594) to have their password reset.

Faculty and staff that require their passwords to be reset should contact Information Systems at 357-5594. Passwords will be reset using the following convention:

"NSUdemons" followed by the first 5 numbers of the SSN

For example John Smith with a SSN of 123-45-6789 would have his password reset to:

NSUdemons12345

Please note that the password is case sensitive.

Student Password Assignments

If a student loses or forgets his/her password, he/she must contact the Student Help Desk to have his/her password reset.

If a student loses or forgets their password, they first should use the password reset feature with the university portal at http://my.nsula.edu/. If the user's security profile has never been setup, the student must contact the Student Help Desk (318-357-6696) to have their password reset.

A student's initial password will be Demons + six digit date of birth

Example: Demons120184

E-mail Policies

University provided e-mail systems are an official means of e-mail communication for faculty, staff, and students. Faculty/staff use of third-party e-mail systems (e.g., Hotmail, Yahoo, AOL, Gmail) are not an acceptable means of communications with students.

The following defines the policies that apply to faculty and staff e-mail:

- NSU provided e-mail is for the conduct of university related business. Any other purpose is strictly forbidden.
- The faculty/staff e-mail client will be Microsoft Outlook or the web-based version of Microsoft Outlook.
- Faculty and staff are responsible for regularly checking their e-mail.
- The Outlook Address List is provided as a convenience for users. This list is not to be used for campus-wide mailings. Campus-wide mailings will be sent using Messenger.

Departmental E-mail

Departmental e-mail accounts provide a means for generic communication with departments without having to know the e-mail address of an individual within the department. Departmental accounts have the advantage of having multiple users who

can access and process the e-mails received (e-mail does not go unanswered if someone is on leave).

The process for obtaining a departmental e-mail account is as follows.

- The department head must submit service request at http://support.nsula.edu/ and provided the following information:
    - Requested name of account (e.g., the school of business may request bussiness@nsula.edu for being the departmental e-mail address.)
    - Short use justification for the account
    - Names of individuals with their user accounts that need access to the shared mailbox
- The CIO or Deputy CIO will give the final approval for all requested departmental accounts

User Policy Summary

Users of University information resources must respect software copyrights and licenses, respect the integrity of computer-based information resources, refrain from seeking to gain unauthorized access, and respect the privacy of other computer users. This policy is applicable to all University students, faculty, and staff and to any others granted use of University resources. This policy refers 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. This includes word processing equipment, personal computers, workstations, mainframes, minicomputers, and associated peripherals and software, regardless of whether used for administration, research, teaching, or other purposes.

Locally Defined and External Conditions of Use

Individual units within the University may define "conditions of use" for information resources under their control. These statements must be consistent with University EDP policy but may provide additional detail, guidelines, and/or restrictions. Where such "conditions of use" exist, enforcement mechanisms defined therein shall apply. The 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. Where use of external networks is involved, policies governing such use also are applicable and must be adhered to.

User Responsibilities

Access to the information 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.

User Accountability

All users are solely accountable for all usage/activity associated with their respective account. This includes any electronic mail, data transfer, Internet sites accessed and personal web pages. Information Systems reserves the right to access the information and/or content related to any user account with justifiable cause. Only the Director of Information Systems can authorize this access.

Governing Policies

Any user of University information resources who is found to have purposely or recklessly violated any of the following policies will be subject to disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action.

Copyrights and Licenses

Copying: All software protected by copyright must not be copied except as specifically stipulated by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied into, from, or by any University facility or system, except pursuant to a valid license or as otherwise permitted by copyright law.

Number of Simultaneous Users: The number and distribution of software 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.

Copyrights: In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is subject to the same sanctions as apply to plagiarism in any other media.

Integrity of Information Resources

Modification or Removal of Equipment: Technology users, including faculty, students, and staff, may not, in any way, modify, dismantle, or remove computer or network equipment, software, or peripherals that are owned by the University/State without proper authorizations. Absolutely no modification may be made to any computer, or peripheral, or network device without the permission of Information Systems and the University Property Control unit.

Encroachment on Access and Use: Computer users must not encroach on others' appropriate access to, or use of, University computer or network devices. 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 by the user to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a University computer or network; and damaging or vandalizing University property.

Unauthorized or Destructive Programs: Computer users must not intentionally develop or use programs which disrupt network or computer use, or which access private or restricted portions of a system and/or damage the software or hardware components of a system. Computer users must use great care to ensure that they do not use programs or utilities that interfere with other computer users or which modify normally protected or restricted portions of the system or user accounts. Computer users must not use network links for any use other than those permitted in the network guidelines.

Academic Pursuits: The University recognizes the value of research on game development, computer security, and the investigation of self-replicating code. The University may restrict such activities in order to protect University and individual computing environments, but in doing so will take account of legitimate academic pursuits.

Unauthorized Access

Abuse of Computing Privileges: Users of University information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable 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 University computing privileges.

Reporting Problems: Any defects or abuse discovered in system accounting or system security must be reported to the appropriate system administrator so that steps can be taken to investigate and solve the problem.

Password Protection: A computer user who has been authorized to use a password-protected account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others.

Privacy

Computer users must respect the privacy of other computer users. The University system provides mechanisms for the protection of private information from examination by others. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to private information are violations of University policy and may violate applicable law. System administrators, with authorization from the Director of Information Systems, may access computer system (not data) files for critical maintenance purposes or in response to suspected policy violations. System administrators will report suspected unlawful or improper activities to the Director of Information Systems.

General: Access to University employee e-mail, class records, research data, manuscripts, and other data, whether created directly by keyboard input or indirectly through analysis by computer programs, is subject to the same presumption of privacy that attaches to material committed to paper, secured in an employee’s office. In extraordinary

circumstances, access to computer records may be granted, with the employee's foreknowledge, by the University President as part of official investigations of misconduct, in response to the written demand of appropriate investigating officials, acting within the scope of appropriate University policies.

Unlawful Messages: Use of electronic communication facilities (such as mail or chat, or systems with similar functions) to send fraudulent, harassing, obscene, threatening, or other messages that are a violation of applicable federal, state, or other law or University policy is prohibited.

Mailing Lists: Users must respect the purpose and charters of computer mailing lists (including local or network newsgroups and bulletin boards). The user of an electronic mailing list is responsible for determining the purpose of the list before sending messages to or receiving messages from the list. Subscribers 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 list's purpose. Persons sending to a mailing list any materials that are not consistent with the list's purpose will be viewed as having sent unsolicited material.

Advertisements/solicitations: In general, the University's electronic communication facilities should not be used to transmit commercial or personal advertisements, solicitations, or promotions (See Commercial Use, below)

Information Belonging to Others: Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users without the permission of the other user and, where applicable, the permission of the system administrator and the Director of Information Systems.

Confidentiality: The University does not exist in isolation from other communities and jurisdictions and their laws. Under some circumstances, as a result of subpoena or lawsuits, individual users or the University may be required by law to provide electronic or other records or information related to those records or relating to use of information resources. In such cases, the Director of Information Systems will immediately inform the President who will in turn notify the Board attorney.

Political, Personal, and Commercial Use

The University is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state, and local laws regarding sources of income, use of real estate, and similar matters. It is also a contractor with government and other entities and thus must assure proper use of property under its control and allocations of overhead and associated costs. Use of the University information resources, including the use of the University computer network capabilities, is, therefore, subject to the following conditions:

Political Use: University information resources may not be used for partisan political activities where prohibited by federal, state, or other applicable laws, and may be used for other political activities only when in compliance with federal, state, and other laws and in compliance with applicable University policies.

Personal Use: University information resources may not be used for personal activities not related to University functions.

Commercial Use: University information resources should not be used for commercial purposes except in a purely incidental manner or as permitted under other written policies of the University or with the written approval of a University officer having the authority to give such approval. Any such commercial use should be properly related to University activities, take into account proper cost allocations for government and other overhead determinations and provide for appropriate reimbursement to the University for taxes and other costs the University may incur by reason of the commercial use. Users also are reminded that the "EDU" domain on the Internet has rules restricting or prohibiting commercial use.

Cause Celebre Use: University information resources may not be used to personally discuss or disseminate information pertaining to matters of public controversy or debate. This restriction is not intended to preclude official or legitimate academic discussion of such matters.

Disruptive Use: University information resources may not be used to disseminate, convey, or solicit information of a disruptive nature to the workplace or classroom (electronic or traditional).

Consequences of Misuse of Computing Privileges

Cooperation Expected

Users, when requested, are expected to cooperate with system administrators in any investigations of system abuse. Users are encouraged to report suspected abuse, especially any damage to or problems with their files. Failure to cooperate may be grounds for cancellation of access privileges or other disciplinary actions.

Corrective Action

If system administrators have persuasive evidence of misuse of computing resources, and if that evidence points to the computing activities or the computer files of an individual, they should pursue one or more of the following steps, as appropriate, to protect other users, data files, and the computer network:

- Provide notification of the investigation to the Director of Information Systems, Vice President of Student Affairs (in the case of student use), the user's instructor, department or division chair, and/or supervisor.
- Temporarily suspend or restrict the user's computing privileges during the investigation. A student may appeal such a suspension or restriction and petition for reinstatement of computing privileges through the Dean of Students. A staff member may appeal through applicable grievance procedures. Faculty members may appeal through the Dean of their college. The Provost, in consultation with the Director of Information Systems, will make final decisions for reinstatement.

- With authorization from the University's Computer Security Officer or designate, inspect the user's files, diskettes, tapes, network use logs, and/or electronic account(s).
- Refer the matter for possible disciplinary action to the appropriate University unit, i.e., the Vice President of Student Affairs for students, the appropriate supervisor for staff, and the Dean of the relevant College for faculty or other responsible teaching or research personnel.

Student Access/Use Policies

The use of University computer/network facilities, including the NSU network, for Internet access, for any reason other than for University related activities, is strictly forbidden. Violators may lose access to University facilities and/or the University network and be subject to state or federal civil or criminal penalties. For policy violations involving a student, referring the case to the Director of Information Systems and to the Vice President of Student Affairs Office is the recommended course of action. This ensures that similar offenses may be considered for similar disciplinary action, from semester to semester, year to year, and instructor to instructor. It also allows the detection of repeat offenders.