

University of Southern Nevada

Computer and Network Acceptable Usage Policy

1. Purpose

University of Southern Nevada technology resources (USNTR) are intended to support and enhance the academic mission and administrative functions of the college. This Acceptable Use Policy (AUP) states the rules and regulations regarding the use of these technologies. This AUP complements and supplements, rather than replaces other policies concerning appropriate conduct of employees and students of University of Southern Nevada. USNTR includes any computer, computer-based network and supporting infrastructure, computer peripheral, e.g. printer, operating system, software or any combination thereof, owned or licensed by University of Southern Nevada or under the custody or control of University of Southern Nevada. This policy also applies to any of the above mentioned items which fall under company and/or personal ownership, used in conjunction with any portions of the University of Southern Nevada networked infrastructure. The college grants access to its networks and computer systems subject to certain responsibilities and obligations set forth herein and subject to all local, state, and federal laws. Appropriate use should always be legal, ethical and consistent with the College's mission, policies, and procedures.

2. Authorized Use

Authorized use of USNTR is use consistent with this policy. An authorized user is any person who has been granted authority by the College to access its technology resources and whose usage complies with this policy. Unauthorized use is strictly prohibited. The term "user" hereinafter refers to any student, staff, faculty member, or anyone affiliated with the University of Southern Nevada.

3. Privacy

Users must recognize that there is no guarantee of privacy associated with their use of USNTR. The College may find it necessary to view electronic data and it may be required by law to allow third parties to do so (e.g. electronically stored data may become evidence in legal proceedings.) It is also possible that messages or data may be inadvertently viewed by others.

4. Individual Responsibilities

4.1. Common Courtesy and Respect for Rights of Others

All users are responsible to respect and value the privacy of others, to behave ethically, and to comply with all legal restrictions regarding the use of electronic data. All users are also responsible to recognize and honor the intellectual property rights of others. Actions or language that constitutes unlawful harassment, threats,

intimidation, defamation, or violence are not permitted. Users who engage in such activity will be subject to disciplinary action.

4.2. Responsible Use

All users are responsible for refraining from all acts that waste USNTR or prevent others from using them. Each user is responsible for the security and integrity of information stored on his/her personal computer. Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with or used by others. All users must maintain confidentiality of student information in compliance with the Family Education Rights and Privacy Act of 1974.

4.2.1. Permitting unauthorized access

All users are prohibited from running or otherwise configuring USNTR to intentionally allow access by unauthorized users.

4.2.2. Termination of access

Whenever a user ceases being a student, staff, or faculty member, or if such user assumes a new position and/or responsibility within the College community, such user shall not use facilities, accounts, access codes, privileges, or information for which he/she is not authorized in his/her new position or circumstances. This includes the return of all USNTR including hardware, software, and peripherals when requested.

4.3. Attempts to circumvent security

Users are prohibited from attempting to circumvent or subvert any security measures implemented for the USNTR. The use of any computer program or device to intercept or decode passwords or similar access control information is prohibited.

4.3.1. Denial of service

Deliberate attempts to degrade the performance of USNTR to deprive authorized users of access to or use of such resources is prohibited.

4.3.2. Harmful activities

The following harmful activities are prohibited: creating or propagating viruses; disrupting services; damaging files; intentional destruction of or damage to equipment, software, or data belonging to the College and the like.

4.4. Use of licensed software

No software may be installed, copied, or used on USNTR except as permitted by the owner of the software and by law. Software subject to licensing must be properly

licensed and all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.) must be strictly adhered to.

4.5. Personal business, political campaigning, and commercial advertising

USNTR are College-owned resources and business tools to be used only by authorized persons for College business and academic purposes. Except as may be authorized by the College, users shall not use USNTR for: compensated outside work and/or the benefit of organizations not related to the College, except in connection with scholarly pursuits (such as faculty publishing and approved consulting activities); political campaigning; commercial or personal advertising; personal gain or benefit of the user.

5. Security

5.1. System administration access

The Director of Technology Services, or his/her designee, will be granted authority to access files for the maintenance of the systems, storage or backup of information, or pursuing system problems. Further, the College may access usage data, such as network session connection times and end-points, CPU and disk utilization, security audit trails, etc. Such activity may be performed within the reasonable discretion of the Technology Resources division management, subject to approval by the President.

6. Procedures and Sanctions

6.1. Responding to security and abuse incidents

All users have the responsibility to report any discovered unauthorized access attempts or other improper usage of USNTR. If a security or abuse problem with any USNTR is observed by or reported to a user, such user shall immediately report the same to Technology Resources division management.

6.2. Range of disciplinary sanctions

Persons in violation of this policy are subject to a full range of sanctions, including, but not limited to, the loss of USNTR access privileges, disciplinary action, and dismissal from the College. Some violations may constitute criminal offenses, as defined by local, state, and federal laws and the College may prosecute any such violation to the full extent of the law.

Printed Name

Signature

Date