SECURITY AWARENESS AND ACCEPTABLE USE POLICY

Overview
The computing resources at the University of Nevada, Reno (UNR) support the educational, instructional, research and administrative activities of the University and the use of these resources are a privilege extended to members of the University community. As a user of these services and facilities, users have access to valuable University resources, to Sensitive Data, and to internal and external networks. Consequently, users of UNR computing resources are expected at all times to behave in a responsible, ethical and legal manner.

Purpose
This Security Awareness and Acceptable Use Policy establishes specific requirements for the use of all computing and networking resources at UNR. Individuals found to be in violation of this Acceptable Use Policy may be subject to disciplinary action in accordance with the University’s applicable disciplinary policies. Users are also required to follow all federal, state and local laws governing information security and use of computing resources, and to follow the University’s Information Security Policies and Procedures (ISPP).

Scope
This policy applies to all users of computing resources owned or managed by UNR. Individuals covered by this policy include, but are not limited to: employees, students, contractors, vendors, third parties and guests accessing services through UNR’s resources. Computing resources include all University owned, licensed, or managed hardware or software, and use of the University network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network. These policies apply to technology administered in individual departments, the resources administered by Information Technology, personally owned computers and devices connected by wire or wirelessly to the campus network, and to off-campus computers that connect remotely to the University’s network.

Policy
Acceptable Use
1. You may only use the computers, accounts, and files for which you have been granted authorization to use.

2. The University is bound by contractual and license agreements respecting third party resources; you are expected to comply with all such agreements while using UNR’s resources.
3. You must make reasonable effort to protect your passwords/credentials and to secure resources against unauthorized use or access. You must configure hardware and software in a way that reasonably prevents unauthorized users from accessing UNR’s network and computing resources.

4. You must comply with the policies and guidelines for any specific set of resources to which you have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

5. Individual departments are responsible for creating guidelines concerning personal use of systems and/or equipment. In the absence of such policies, in accordance with NRS 281A.400 limited use for personal purposes is allowable if the use does not interfere with the performance of an employee’s duties, the cost and value related to use is nominal, and the use does not create the appearance of impropriety or of endorsement by the University or Nevada System of Higher Education. If there is any uncertainty, employees should consult their supervisor or manager.

Security
1. Users with access to data contained on UNR’s systems that is classified as Confidential or Regulated must take all necessary precautions to prevent unauthorized access to this information. Examples of Confidential or Regulated Data include but are not limited to Family Educational Rights and Privacy Act (FERPA), Graham Leach Bliley Act (GLBA), proprietary, Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), and confidential research data.

2. Employees should secure their workstations by logging off or locking when the host will be unattended.

3. Because information contained on portable devices is especially vulnerable, special care should be exercised. Protect laptops in accordance with current security standards, including personal firewalls.

4. Postings by employees from a UNR email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of UNR, unless posting is in the course of business duties.

5. All hardware used by the employee that is connected to the UNR network, whether owned by the employee or by UNR, shall be continually executing approved virus-scanning software with a current virus database.

6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code and/or may be considered “phishing”.

Prohibited Actions
The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
Under no circumstances is a user of UNR computing resources authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing UNR-owned or managed resources. The list below is by no means exhaustive, but provides a framework for activities which fall into the category of prohibited actions.

1. Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by UNR.

2. All users must comply with the Digital Millennium Copyright Act (DMCA). Unauthorized copying of copyrighted material including, but not limited to, digitizing and distributing of photographs from magazines, books or other copyrighted sources, copyrighted music, television or movies, and the installing of any copyrighted software for which UNR or the end user does not have an active license is strictly prohibited.

3. The use of any University owned recording device such as, but not limited to, digital cameras, video cameras, and cell phone cameras, on the University campus shall comply with NRS 396.970.

4. Connecting network devices such as wireless access points or personal laptops into the UNR network environment without proper authorization from Information Security.

5. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. Research Compliance should be consulted prior to export of any material that is in question.

6. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

7. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

8. Using a UNR computing asset to actively engage in conduct that is in violation of sexual harassment or hostile workplace laws.

9. Making fraudulent offers of products, items, or services originating from any UNR account.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior authorization is gained by Information Security.

12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

13. Circumventing user authentication or security of any host, network or account.

14. Attempting to access restricted portions of the network, an operating system, security software, or other administrative applications without appropriate authorization from the system owner or administrator.

15. Intentionally accessing another person’s account or email without authorization, or attempting to capture or guess other user’s passwords.

16. Sending “spam”, chain letters, or any other type of widespread distribution of unsolicited communications unrelated to the sender’s University related duties.

17. Use of email for commercial activities, or personal or financial gain, unless and solely to the extent otherwise permitted by NRS 281A.400(7).

18. Sending of messages that violate any applicable University or Nevada System of Higher Education policy.

19. Unauthorized use, or forging, of email header information, or impersonation of another person’s email account.

Privacy
While the University desires to provide a reasonable level of privacy and does not generally monitor or limit content of information transmitted on the campus network, it reserves the right to access and review such information under certain conditions. These include the following: investigating performance deviations and system problems (with reasonable cause), determining if an individual is in violation of this policy, as may be authorized by other University or NSHE policy, or, as may be necessary to ensure that UNR is not subject to claims of institutional misconduct.

1. For security and network maintenance purposes, authorized individuals within UNR may monitor equipment, systems and network traffic at any time. UNR reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2. In the event of a legal proceeding or as otherwise authorized by the President of the University (or designee), under the advisement of the Office of General Counsel, Information Security reserves the right to access and inspect stored information without the consent of the user when the information is stored within UNR computing resources.

3. As a public agency, UNR is subject to Public Records requests (Nevada Revised Statutes chapter 239). Users that have University records contained in their personal email accounts or on personal devices are responsible for furnishing such information when requested under these laws.