



OFFICE OF INFORMATION TECHNOLOGY

ACCEPTABLE USE OF COMPUTING AND INFORMATION TECHNOLOGY RESOURCES POLICY

RESPONSIBLE ADMINISTRATOR: VICE PROVOST FOR INFORMATION TECHNOLOGY
RESPONSIBLE OFFICE(S): OFFICE OF THE VICE PROVOST FOR INFORMATION TECHNOLOGY
ORIGINALLY ISSUED: DECEMBER 2013
APPROVALS:

APPROVED BY: [Signature] 12/16/13
Lori L. Temple, Vice Provost for Information Technology Date

APPROVED BY: [Signature] 12/16/13
John Valery White, Executive Vice President & Provost Date

APPROVED BY THE PRESIDENT: [Signature] 12/16/13
Neal J. Smatresk Date

REVISION DATE: NA

STATEMENT OF PURPOSE

The purpose of this policy is to:

- Ensure that use of computing and information technology resources is consistent with the principles and values of the university including academic freedom, privacy, and security.
Ensure that computing and information technology resources are used for their intended purposes and meet compliance requirements.
Ensure the confidentiality, integrity, availability, reliability and proper performance of computing and information technology resources.

ENTITIES AFFECTED BY THIS POLICY

Entities affected by this policy include UNLV students and employees and anyone who accesses UNLV computing and/or information technology resources.

WHO SHOULD READ THIS POLICY

UNLV students and employees and anyone who accesses UNLV computing and information technology resources should read this policy.

THE CONTEXT

UNLV's computing and information technology resources are dedicated to the support of the university's mission and its core themes to promote student learning and success, advance and support research scholarship, and creative activity, and foster inclusion and community engagement. While advancing the mission and core themes, UNLV respects, upholds, and endeavors to safeguard the principles of academic freedom, freedom of expression, and freedom of inquiry. UNLV's commitment to the principles of academic freedom and freedom of expression includes electronic information.

The use of computing and information technology resources in a manner consistent with the mission and ideals of the university and with the Nevada System of Higher Education (NSHE) Computing Resources Policy requires adherence to legal statutes, approved policies, and responsible behavior, including:

- using only assigned account(s) or account information
- respecting the privacy and rights of other computer users
- protecting the integrity of the physical environments in which information technology equipment resides
- complying with all pertinent software license and contractual agreements, and
- obeying all UNLV and NSHE regulations, state and federal laws.

UNLV seeks to create an atmosphere of privacy with respect to information and UNLV information technology resources. UNLV acknowledges its responsibilities to respect and advance free academic inquiry, free expression, reasonable expectations of privacy, due process, equal protection of the law, and legitimate claims of ownership of intellectual property. Such responsibilities are balanced with the acknowledgement that users should be aware that they should have no expectation of privacy in connection with the use of UNLV resources beyond the explicit provisions of university policy and applicable federal and state law (e.g., NRS Chapter 239, Public Records). UNLV is a public institution, and because the university must be able to respond to lawful requests and ensure the integrity and continuity of its operations, use of the university's information resources cannot be completely private.

Information on university computers and equipment may be subject to legal discovery and disclosed:

- In response to lawfully executed court ordered warrants or subpoenas
- As a result of the Nevada Public Records Act (i.e. public records request)
- In response to federal “Freedom of Information Act” requests
- In litigation involving the university and/or university employees
- In criminal investigations or investigations of student or employee misconduct
- In university investigations in accordance with NSHE or university policy.

When warranted, university staff are asked to assist in investigations and discovery and have direct responsibility for investigating and responding to some alleged offenses and incidents involving computing resources.

POLICY

1. Each person may use only those computing and information technology resources for which he or she has authorization.

Examples of violations include, but are not limited to:

- a) asking another person for individual account passwords or attempting to obtain such passwords by any means
- b) using resources without authorization
- c) sharing university accounts with other persons without authorization
- d) accessing files, databases, data or processes without authorization
- e) using former system and access privileges without authorization after association with the university has ended.

2. Computing and information technology resources must be used in a manner that respects the privacy and rights of others.

Examples of violations include, but are not limited to:

- a) accessing, attempting to access, or copying someone else’s electronic mail, data, programs, or other files without authorization
- b) divulging sensitive, personal information without a valid business or academic reason
- c) developing or using programs that may cause problems or disrupt services for other users
- d) misrepresenting another user’s identity in any electronic communication (e.g., forging an e-mail address)
- e) using electronic resources for deceiving, harassing or stalking other individuals

- f) sending threats, “hoax” messages, chain letters, or phishing
- g) intercepting, monitoring, or retrieving any network communication without authorization.

3. The access to and integrity of computing and information technology resources must be protected.

Examples of violations include, but are not limited to:

- a) sharing passwords
- b) purposefully propagating computer malware such as computer viruses, worms or Trojan Horses, except under secure conditions for research or teaching purposes
- c) preventing others from accessing an authorized service
- d) degrading or attempting to degrade performance or deny service
- e) corrupting information
- f) altering or destroying information without authorization
- g) making university systems and resources available to those not affiliated with the university
- h) installing hacking or vulnerability tools in university systems without authorization
- i) circumventing or attempting to circumvent security mechanisms without authorization.

4. Applicable laws and university policies must be followed.

Examples of violations include, but are not limited to:

- a) uploading, downloading, distributing or possessing material deemed illegal under US and state laws, such as child pornography or classified information
- b) using university computing or network resources for advertising, partisan political activities or commercial purposes (see the exception for “UNLV Student elections, which are governed by CSUN policy” in Section II.1. “Partisan Political Activity” and the definition of political activity from the NAC 284.770, both referenced in the Related Documents section)
- c) making unauthorized copies of licensed software
- d) downloading, using or distributing illegally obtained media (e.g., software, music, movies) using the campus network, whether on a UNLV-issued computer or not
- e) accessing, storing or transmitting sensitive, personal information without a valid business or academic reason, or outside the parameters of limited personal use
- f) transmitting sensitive, personal information without using appropriate security protocols (NRS 603A).

5. Limited personal or non-university use of UNLV computing and information technology resources is allowable only if ALL of the following conditions are met:

- a) the use does not interfere with an employee's duties
- b) the cost and value related to use is nominal
- c) the use does not create the appearance of impropriety or UNLV endorsement
- d) the use is otherwise consistent with this policy.

Refer to the Office of Information Technology's Policies and Procedures web page at <https://www.it.unlv.edu/policies> for additional information, including how to request an exception to this policy.

RELATED DOCUMENTS

Nevada System of Higher Education (NSHE) Computing Resources Policy. NSHE Title 4, Chapter 1, Section 23

<https://nshe.nevada.edu/wp-content/uploads/file/BoardOfRegents/Handbook/COMPLETEHANDBOOKREV282.pdf>

Guidelines for Scheduling University Facilities, Section II, 1, Partisan Political Activity

<https://www.unlv.edu/campuslife/scheduling-guidelines>

Nevada Administrative Code, 284.770 – Political activities

<http://www.leg.state.nv.us/nac/NAC-284.html#NAC284Sec770>

Nevada Revised Statutes, Chapter 603A – Security of Personal Information

<http://www.leg.state.nv.us/NRS/NRS-603A.html>

Nevada Revised Statutes, Chapter 239, State of Nevada Public Records Law

<http://www.leg.state.nv.us/nrs/nrs-239.html>

CONTACTS

Refer to the Office of Information Technology's Policies and Procedures web page at <https://www.it.unlv.edu/policies> for a list of individuals who can answer questions about the policy.

DEFINITIONS

These definitions apply to these terms as they are used in this policy.

Authorization - Permission to engage in activities otherwise deemed unacceptable only if required by existing policies, procedures, documented approval, assigned responsibility, or

research or teaching purposes with adequate protections and in accordance with federal, state, and local laws.

Phishing - A scam by which an e-mail user is duped into revealing sensitive, personal or confidential information, which the scammer can use illicitly.

Sensitive, personal information - Any information about the individual maintained by the university, including the following: (a) Education, financial transactions, medical history, and criminal or employment history; and, (b) Information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records.

Student - Currently admitted to UNLV - or - enrolled in at least one course at UNLV - or - has completed at least one course at UNLV within the previous six academic semesters (spring, summer, and fall).

Systems - Devices and applications accessed via the network.