



OFFICE OF INFORMATION TECHNOLOGY

IST POLICY 101A: ACCEPTABLE USE POLICY FOR USERS

RESPONSIBLE ADMINISTRATOR: VICE PROVOST FOR INFORMATION TECHNOLOGY
RESPONSIBLE OFFICE(S): OFFICE OF INFORMATION TECHNOLOGY
ORIGINALLY ISSUED: APRIL 2007
APPROVALS: APPROVED BY THE EXECUTIVE VICE PRESIDENT AND PROVOST:

Neal J. Smatresk *Date*

APPROVED BY THE PRESIDENT:

David B. Ashley *Date*

REVISION DATE: 15-JAN-09
POLICY REVIEW PERIOD: SEMI-ANNUALLY **SECURITY RESPONSE PRIORITY LEVEL:** (TBD)

STATEMENT OF PURPOSE

The purpose of this policy is to provide management direction and support for information security in accordance with business requirements and relevant State and Federal laws and regulations. This policy, in conjunction with the other IT security policies, defines the acceptable use of UNLV information technology services and accounts.

ENTITIES AFFECTED BY THIS POLICY

This policy impacts all Academic Colleges, Schools and Departments, and all faculty, staff, students, and contractors at all levels.

WHO SHOULD READ THIS POLICY

This policy should be read by all members of the campus community, all entities that do business with the University, as well as periodic and one-time visitors to UNLV.

POLICY

Establishment of UNLV computer and network accounts, and acceptable usage shall be governed by the standards and procedures set forth in this policy and NSHE Computing Resources Policy. Computer and network systems may be used only for their authorized purposes -- that is, to support the research, education, clinical, administrative, scholarly and creative production, and other functions of the

University. The particular purposes of any of these systems as well as the nature and scope of authorized incidental personal use may vary according to the duties and responsibilities of the User. The legitimate use of a computer or network system does not extend to whatever an individual is capable of doing with the system. Although some restrictions may be a part of the management of a system, even the best management strategies cannot limit completely what an individual can do or can see. Each member of the community is responsible for his/her actions whether or not rules are built in, and whether or not they can be circumvented.

SCOPE AND APPLICABILITY: The policy applies to the access to, use of, maintenance, review, and disclosure of various electronic communications, including those sent or received by users on UNLV IT systems and networks.

The information technologies covered by the policy include systems, networks, and facilities administered by OIT, as well as those administered by individual schools, departments, University laboratories, and other university-based entities.

Use of IT systems, even when carried out on a privately owned computer that is not managed or maintained by UNLV, is governed by this policy. OIT adheres to a set of practices and standards in accordance with the NSHE Computing Resources Policy to fulfill the tasks of administering and securing these systems and networks.

UNLV has established specific guidelines, and procedures, outlined in this document, to be used by all members of the University for implementation and legal compliance of processes to be used for the purpose of maintaining an orderly use and conducting university actions necessary for computer security. This policy applies to all UNLV electronic systems and also privately owned electronics that are attached to the UNLV network.

The determination of whether a staff, faculty, or other member of UNLV will be allowed to request access to another person's or entity's computer account will be made on a case-by-case basis in accordance with the UNLV IT Policy on ***Access to Non E-Mail Accounts***.

The determination of whether a staff, faculty, or other member of the UNLV community is improperly using or abusing their privileges will be made on an individual basis in accordance with the policies and processes outlined. If a person has a dispute regarding a decision under this policy, it should be brought, first, to the attention of the Office of Information Technology. If the resolution does not seem adequate, then the concern should be brought to the attention of the UNLV Provost.

In order to manage information technology comprehensively, the UNLV OIT Acceptable Use Policy serves to protect the established and legitimate acceptable use, information privacy, and security of all members of the UNLV community while providing management and system administrators policies to support the performance of their university assigned duties. This portion of the policy, Part A, is written for users while Part B is written for IT managers and system administrators. Other than the policy statements, most sections in the two parts are identical.

For more assistance, contact the appropriate office representative listed in the [Contacts](#) section of this document.

BACKGROUND: The UNLV Office of Information Technology (OIT) maintains the UNLV campus-wide network environment that delivers Internet access, core security services, integrated email, and related application services to meet the administrative, academic, privacy, and research needs of the UNLV campus community. This policy is established to ensure an information technology infrastructure that promotes the missions of the university. In particular, this policy aims to promote the following goals:

- To ensure that use of IT systems is consistent with the principles and values of the university including privacy, security, and academic freedom
- To ensure that IT systems are used for their intended purposes and meet any compliance requirements;
- To ensure the confidentiality, integrity, availability, reliability, and superior performance of IT systems; and
- To establish processes for addressing policy violations and sanctions for violators.

The University seeks to

- Enforce its policies regarding privacy, harassment, and the safety of individuals;
- To protect the university against seriously damaging or legal consequences;
- To prevent the posting of proprietary software or the posting of electronic copies of literary and other works in disregard of copyright restrictions or contractual obligations;
- To safeguard the integrity of computers, networks, and data, either at UNLV or elsewhere;
- To ensure that use of electronic communications complies with the provisions of the NSHE Code, UNLV Bylaws, and Student Code of Conduct for maintaining public order or the educational environment;
- To ensure that management and system administrators are authorized to perform their university assigned duties and are bound by the same codes; and
- To prevent disruptions to and misuse of University electronic communications resources, services, and activities.

POLICY STANDARDS AND CONTROLS: See the ANNEX below titled STANDARDS for mandatory baseline Policy Standards and Controls that are required to be implemented to be in minimum compliance with this policy and its objectives.

COMPLIANCE: It is the responsibility of the UNLV Provost OIT to administer and maintain this Policy and all related information security policies. The Policy shall also be maintained and enforced with assistance from the UNLV Provost, UNLV Office of General Counsel, and NSHE System Computing Services (SCS). Policy compliance requirements are:

1. UNLV management has the responsibility to manage University information, personnel, and physical property relevant to academic and business operations, as well as the right to monitor the actual utilization, but not the content except under pre-approved conditions, of all University assets.
2. Information security reviews and security audits will be conducted annually or more frequently as required. The UNLV Information Security Officer, or appointed designee, will conduct security policy reviews and security audits.

3. Components of this policy are drawn from Nevada State Codes and Statutes, NSHE Board of Regents Handbook, and “accepted best practices” across the IT industry. Members of the University community also are expected to follow all other policies, rules, or procedures established for the orderly use and protection of email systems, including UNLV and NSHE policies:
4. In addition to any possible legal sanctions, UNLV employees and students who fail to comply with the policies will be considered in violation of the University's relevant codes of conduct and may be subject to disciplinary action up to and including dismissal or expulsion, pursuant to Campus policies, collective bargaining agreements, codes of conduct, or other instrument governing the individual’s relationship with the University. Recourse to such actions shall be as provided for under the provisions of those instruments.

AUDIT STANDARDS AND CONTROLS: Compliance and effectiveness auditing of this policy shall be accomplished using the appropriate BS 7799.2:200x Audit Check List, dated 8.08.2005 or later, and through a complete review of all related misuse complaints (security incidents) that occurred after the previous audit. The audit shall inspect the in-use security applications, procedures, and processes of systems supporting this policy, including timeliness of updates, for compliance to the policy. The UNLV ISO, or designee, shall be the ombudsman, manager and principal reviewer of this policy. Proposed adjustments and enhancements to the policy for unforeseen issues shall be presented to the Responsible Administrator of this Policy for approval. An audit report and recommendations shall be sent to the Vice Provost for Information Technology.

ROLES AND RESPONSIBILITIES: See the ANNEX for ROLES AND RESPONSIBILITIES for the policy responsibilities of Administrative Officials, IT Providers, and Users.

USER EXPECTATIONS AND NOTICES

The use of computers or network systems does not exempt any member of the university community from the normal requirements of ethical or legal behavior at UNLV. In particular, data, software, and computer capacity are considered critical assets of UNLV, have value and must be treated accordingly. Use of a computer and network system that is shared by many users imposes certain additional obligations. Although this policy sets forth the general appropriate use of IT systems, UNLV users should consult their respective department IT policy manuals, if any, for more detailed statements on permitted use and the extent of use that the University considers appropriate in light of their differentiated roles within the community.

Members of the university community are expected to follow principles of ethical behavior in making use of computers and network systems, in particular, to respect, and to observe policies and procedures governing:

- the privacy of or other restrictions placed upon data or information stored in or transmitted across computers and network systems, even when that data or information is not securely protected;
- an owner's interest in proprietary software or other assets pertaining to computers or network systems, even when such software or assets are not securely protected;
- the finite capacity of computers or network systems by limiting use of computers and network systems so as not to interfere unreasonably with the activity of other Users.

Members of the University community also are expected to follow all other policies, rules, or procedures established for the orderly use and protection of digital systems, including UNLV and UCCSN policies. See the "Quick Links" section below for web access.

MONITORING, NON-COMPLIANCE AND EXCEPTIONS

MONITORING (VIOLATIONS): Authorized Access and Violations - Access to electronic communications is limited to that authorized by the system authority. Each member of the University community is responsible for his or her actions in the use of the University IT systems. Should it become necessary to authorize action that would restrict, prevent and/or grant access to the information contained in a computer or network account without the accountholder's consent, the procedures and steps detailed in the UNLV Digital Investigation and Security Incident Handling Policy will be followed by the Office of Information Technology to comply with the request. In the event that any person required by this process is unable or disallowed to act as required by the process, the nearest available official in that person's chain of command shall act on their behalf within the defined guidelines. All steps in the processes are to be conducted in the strictest of confidence. Written requests and authorizations are preferred but may be filed via email if prior approval for such submission is given.

It is an explicit violation of this policy to do any of the following:

1. Knowingly or intentionally compromise an account, network, system, or database.
2. Knowingly or intentionally use the email system to engage in cyberstalking or any form of cyberharassment of an individual.
3. Knowingly or intentionally attach mis-configured IT devices to the network.
4. Knowingly or intentionally compromise an email system.
5. Knowingly or intentionally maintain insecure passwords on IT devices attached to the network (e.g., absence of administrative password, password written and stored in insecure location, shared passwords, etc.) Knowingly or intentionally compromise an IT device attached to the network or intentionally use an application or computing system with a known compromise.
6. Knowingly or intentionally, (or negligently after receiving notice from an information technology officer or professional), transmit any computer virus or other form of malicious software.
7. Knowingly or intentionally access or exploit resources for which you do not have authorization.
8. Knowingly or intentionally perform network or system scans on resources not authorized by the IT Security Director, unit head, unit security liaison, or local support provider.
9. Knowingly or intentionally fail to implement the security policies and directives related to the IT resources for which you control or administer.

10. Knowingly or intentionally perform network or system email interception or account monitoring not assigned to you or properly authorized.
11. Knowingly or intentionally divulge or otherwise communicate information concerning UNLV investigations or information collected to any person not authorized for access to that information.

NON-COMPLIANCE (ENFORCEMENT): Suspected policy violations will be investigated by the UNLV IT Security Officer. Disciplinary actions may be taken in accordance with the NSHE, UNLV Bylaws, and Student Code of Conduct applicable regulations, or other university policies.

Filing Complaints of Alleged Violations. An individual who believes that he or she has been harmed by an alleged violation of this policy may file a complaint in accordance with established university procedures (including, where relevant, those procedures for filing complaints of sexual harassment or of racial or ethnic harassment) for students, faculty, and staff. The individual is also encouraged to report the alleged violation to the Systems Authority overseeing the facility or systems most directly involved, or to the UNLV Information Security Office, which must investigate the allegation and (if appropriate) refer the matter to university disciplinary and/or law enforcement authorities.

Reporting Observed Violations. If an individual has observed or otherwise is aware of a violation of this policy, but has not been harmed by the alleged violation, he or she may report any evidence to the Systems Authority overseeing the facility or systems most directly involved, or to the UNLV Information Security Office, which must investigate the allegation and, if appropriate, refer the matter to university disciplinary and/or law enforcement authorities.

Disciplinary Procedures. Alleged violations of this policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students. The IT Security Officer will refer these cases for disciplinary action to the following officers:

- If the alleged violator is a student, the Student Conduct Officer.
- If the alleged violator is a classified staff employee, Human Resources.
- If the alleged violator is a professional staff employee, the Administrative Code Officer.

Systems administrators and the Information Security Office may participate in the disciplinary proceedings as deemed appropriate by the relevant disciplinary authority.

Guest privileges. Violation of UNLV IT policy may result in the revocation of guest privileges.

Legal Liability for Unlawful Use. In addition to University discipline, users may be subject to criminal prosecution, civil liability, or both for unlawful use of any university IT system.

EXCEPTIONS: (None)

RELATED DOCUMENTS

UNLV IT POLICIES -Information security policy structure is based on:

- ISO 17799/27001 – the International Standard for Information Security, and

- enhanced as needed by the [Federal Information Processing Standards \(FIPS\) Pub 199](#) Standards for Security Categorization,
- the *National Institute of Standards and Technology (NIST) Special Publication 800-series* reports on the Information Technology Laboratory's research related to information security controls, standards, and guidelines.
- The standard reference text for ISO 17799/27001 policy development is the most current edition of *Information Security Policies and Procedures: a practitioner's reference*, Thomas R. Peltier, Auerback Publications or it's replacement.

QUICK LINKS:

- UNLV Acceptable Email Usage Policy http://www.unlv.edu/infotech/IT_Policies/Policy_1.03_Email_Usage.html;
- NSHE Computing Resources Policy <http://www.scs.Nevada.edu/about/policy061899.html>;
- UNLV Faculty Computer Use Policy <http://www.unlv.edu/infotech/itcc/FCUP.html>; and
- UNLV Student Computer Use Policy <http://ccs.unlv.edu/scr/computeruse.asp>

SERIES IS – CAPSTONE POLICIES GROUP (Tier 1)

Policies that establish the foundation for information security and information assets policies.

<i>IS01 Information Security for IT Resources Policy**</i>
<i>IS02 Information Sensitivity and Classification Policy (with Handbook)**</i>
<i>IS03 Personal Non-Public Information Policy**</i>
<i>IS04 Infrastructure Responsibilities and Services Policy**</i>

SERIES IST100 - INDIVIDUAL PRIVILEGES & RESPONSIBILITIES GROUP (Tier 2)

Policies that address acceptable personal use of the computing services, assets, and networks.

<i>101A Acceptable Use of IT Resources Policy (Users)**</i>
<i>101B Acceptable Use of IT Resources Policy (Mgmt & SysAdmin)**</i>

BEST SECURITY PRACTICES SERIES

- BSP-1 Password Standards For Personal Systems (With Guide)**
- BSP-2 IT Server Resources Used For Unrestricted Information**
- BSP-3 Password Standards For Servers And Network Devices**
- BSP-4 Virus, Trojan, Spyware & Other Malicious Code Prevention**
- BSP-5 Reporting Electronic Security Incidents**
- BSP-6 What To Do For A Computer Security Incident (For System And Security Administrators)**
- BSP-7 Computer Security Of User Systems**
- BSP-8 Data Media Sanitization & Destruction**
- BSP-9 IT Resources Requiring Compliance Protection For Sensitive, Critical, Or Regulatory Information**

The following Best Security Practices are, fully or partially, restricted because of content, have limited distribution to system and security administrators, and are only available via internal UNLV mail by contacting the UNLV Information Security Office for further information and prerequisite requirements.

BSP-2(R) IT Server Resources Used For Unrestricted Information

- BSP-3(R)** *Password Standards For Servers And Network Devices*
BSP-6(R) *What To Do For A Computer Security Incident (For System And Security Administrators)*
BSP-9(R) *IT Resources Requiring Compliance Protection For Sensitive, Critical, Or Regulatory Information*
BSP-9(R)A *IT Resources Requiring Compliance Protection For Sensitive, Critical, Or Regulatory Information (Supplement)*
BSP-10(R) *Critical Network Resources*
BSP-10(R)A *Critical Network Resources Supplement*
-

CONTACTS

OFFICE OF INFORMATION TECHNOLOGY
Herman W Westfall (HWB), Room 101
(702) 895-3628 / FAX (702) 895-1847

Subject	Contact	Telephone	Email/URL
Initial Contact for Questions	Local System Provider	System-specific	
Policy Clarification	Office of Information Technology	(702) 895-0500	http://www.UNLV.edu/infotech/policy.html
Legal Issues	Administrative Code Officer	(702) 895-1879	- none -
Information Security	Information Security Officer	(702) 895-5284	informationsecurityoffice@unlv.edu
Campus Computing Services	Director of Campus Computing Services	(702) 895-0787	- none -
Enterprise Applications Services	Director of Systems & Applications	(702) 895-1765	- none -
Security of Network Systems	Network Operations Center (NOC)	(702) 895-0760,	- none -
Security of Enterprise Applications Systems	Applications Security or Systems Manager or IT Security Officer	(702) 895-4641, (702) 895-1667	- none -

DEFINITIONS

Key Definitions for this policy:

Account Owner: the individual or office that was assigned the account and normally is the primary user of the IT account. The individual or office with the assigned account password and authorized to change the password.

Additional Definitions of terms in this and other policies can be found in UNLV OIT document "*Information Security Acronyms, Terms and Definitions*".

ANNEX-1: POLICY STANDARDS

BASELINE SECURITY STANDARDS AND CONTROLS. The following are the Policy Standards that shall be implemented to be in minimum compliance with the Policy and its objectives. *Each impacted UNLV organization is responsible for development of internal procedures and directives to implement and comply with this policy for their organization.*

The Office of Information Technology will not comply with a request to take action regarding any accountholder's account on any UNLV or NSHE-owned system without appropriate authorization.

In the event of conflict between UNLV IT policies, this Appropriate Use Policy will prevail.

POLICY STANDARD: 1.01-1 Authorized Users. Authorized and authenticated Users are entitled to access only those elements of computer and network systems that are consistent with their authorization.

POLICY STANDARD: 1.01-2 Personal Account Responsibility. Users are responsible for maintaining the security of their own IT systems accounts and passwords. Any User changes of a password must follow published guidelines for passwords. Accounts and passwords are normally assigned to single Users and are not to be shared with any other person without authorization by the applicable Systems Administrator. Users are presumed to be responsible for any activity carried out under their IT systems accounts or any information posted on their personal web pages.

POLICY STANDARD: 1.01-3 Authorized Access to Stored Content. All digital information stored on UNLV systems will be divulged to law enforcement at the discretion of appropriate UNLV authorities in accordance with the Digital Investigation & Security Incident Handling Policy.

POLICY STANDARD: 1.01-4 Responsibility for Content. Official university information may be published in a variety of electronic forms. The Certifying Authority under whose auspices the information is published is responsible for the content of the published document. Users also are able to publish information on IT systems or over UNLV's networks. Neither UNLV nor individual Systems Administrators can screen such privately published material nor can they ensure its accuracy or assume any responsibility for its content. The university will treat any electronic publication provided on or over IT systems that lacks a Certifying Authority as the private speech of an individual.

POLICY STANDARD: 1.01-5 Personal Identification. Users of UNLV IT resources, if requested in person by a Systems Administrator or other University authority, must produce valid university identification or appropriate guest authorization. If requested via telephone, in response to a "help desk" call, users must provide the requested personal information excluding any disclosure of their full social security number (SSN).

POLICY STANDARD: 1.01-6 Accusatory Knowledge. Knowledge of accusations or investigations of alleged misuse or abusive conduct must be kept strictly confidential.

POLICY STANDARD: 1.01-7 Unacceptable Acts. Any act or conduct not elsewhere defined that obstructs or hinders the application and enforcement of the UNLV OIT IT Policies is prohibited.

POLICY STANDARD: 1.01-8 Unacceptable Use of IT Systems. The following activities are, in general, prohibited. Selective UNLV personnel may be exempt 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 anyone authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing UNLV-owned resources.

System and Network Activities

Examples of activities which fall into the category of unacceptable use:

- a. Violations of 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 UNLV or the individual.
- b. Unauthorized release, publication, or transmission, or causing the same, of any privacy, "sensitive", or restricted information that violates compliance of UNLV, NSHE Board of Regents, local, state, or federal codes, laws, or regulations.
- c. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of content from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which UNLV or the User does not have an active license is strictly prohibited. Refer to UNLV Copyright Policies.
- d. Using a UNLV computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace policies or laws.
- e. Using UNLV IT resources for harassing, cyberharassing, stalking, cyberstalking, or threatening use is strictly prohibited. This category includes, for example, display of offensive, sexual material in the workplace and repeated unwelcome contacts with another. Refer to the UCCSN Sexual Harassment Policy and Complaint Procedure.
- f. 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.
- g. Obtaining, possessing, using, or attempting to use someone else's password regardless of how the password was obtained.
- h. Circumventing User authentication or security of any host, network or account.
- i. Unauthorized access to data or files even if they are not securely protected (e.g., breaking into a system by taking advantage of security holes, or defacing someone else's web page).
- j. Intercepting digital telephonic or network transmissions, including wireless transmissions (e.g., running network sniffers without authorization).
- k. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of assigned responsibilities. 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.
- l. Scanning of computer ports or security settings is expressly prohibited unless appropriate information technology authority's authorization is obtained.
 - m. Introducing malicious programs or malware into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
 - n. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a User's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
 - o. Interfering with or denying service to any User other than the User's host (for example, denial of service attack).
 - p. Making fraudulent offers or fraudulent purchases of products, items, or services originating from any UNLV network or system account.
 - q. Providing information about, or lists of, UNLV employees to parties outside UNLV unless authorized to do so.
 - r. Exporting software, technical information, encryption software or technology, in violation of international or U.S. export control laws. Such activity is illegal.
 - s. Using IT systems in a way that suggests University endorsement of any political candidate or ballot initiative is also prohibited. Users must refrain from using IT systems for the purpose of lobbying that connotes University involvement, except for authorized lobbying through or in consultation appropriate with legal counsel.
 - t. Using IT systems in a way that may cause harm to other IT systems or to the integrity of any State of Nevada institution.

Email and IT Communications Activities

Complete coverage of email and IT communications policies are contained in the UNLV Email Usage Policy and the UNLV Access to Email Accounts Policy. Examples of activities which fall into the category of unacceptable use include:

- a. Sending or forwarding non-UNLV (e.g., non-University related) unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam). Normal University person-to-person, department-to-person, or UNLV-to-person email communications are exempt.
- b. Any form of harassment, cyberharassing, stalking, cyberstalking, or threats via messaging or email, whether through image, language, frequency, or size of messages.
- c. Unauthorized use, or forging, of email header information.
- d. Soliciting or subscribing to an email service using another person's email address with the intent to harass or to collect replies.
- e. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- f. Posting the same or similar messages to large numbers of newsgroups (i.e., newsgroup spam).

POLICY STANDARD: 1.01-9 Responsibility to Cooperate. All users have a responsibility to cooperate and to respond to questions associated with internal investigations.

POLICY STANDARD: 1.01-10 Investigative Contact. If anyone is contacted by a representative from an external law enforcement organization, e.g., FBI, Metro Police Department, etc., that is conducting an investigation of an alleged violation involving UNLV computing and networking resources, he or she must inform the UNLV Office of Information Technology and the UNLV Administrative Code Office immediately. Refer the requesting agency to the Associate Provost for OIT; that Office will provide guidance regarding the appropriate actions to be taken.

SUPPLEMENTAL *Directives, Procedures, Handbooks, and Guidelines*, if included, are located in the last section or appendices of the document.

ANNEX-2: ROLES AND RESPONSIBILITIES

ACCOUNTABILITY:

Obligations of the User

Any individual who uses an IT device and has a UNLV computer or network account (see the "Definitions" section of this document) is a user.

The user is responsible to do the following:

1. Understanding and complying with current policies, requirements, guidelines, procedures, and protocols concerning the university electronic networks, devices, software, and email.
2. Complying with guidelines and practices established by OIT and the local system provider.
3. Updating campus-wide security applications, including anti-virus software and operating system updates, in a timely fashion.
4. Protecting the resources under his or her control by using appropriate passwords.
5. Contacting the local system provider or the CCS Help Desk whenever a questionable situation arises regarding the security of the service.
6. Reporting all electronic security incidents, threats, or harassment to the local system provider or the University Information Security Office immediately, as detailed in University Policy.
7. Assisting in the performance of remediation steps in the event of a detected vulnerability, infection, or compromise.

Obligations of Local System and Email System Providers

A local system/email system provider is the organization with principal responsibility for the installation, configuration, security, and ongoing maintenance of an IT device(s) (e.g., system administrator, network administrator, etc.).

The local system provider is responsible to do the following:

1. Be knowledgeable and comply with the current policies, requirements, guidelines, procedures and protocols concerning the administration and security of the University information technology resources.
2. Follow appropriate best practices guidelines for configuring and maintaining IT systems.
3. Understand and document the specific configurations and characteristics of the service he or she supports to be able to respond to information technology threats and to support recovery and mitigation efforts appropriately.

4. Understand and recommend the appropriate measures to provide security to the resources under his or her control, including, but not limited to:
 - a. physical security to protect resources such as keys, doors and/or rooms maintained to the level of security commensurate with the assigned value of the resources stored in those locations.
 - b. administrative security to protect resources such as:
 - full implementation of the most current authentication and authorization technologies utilized by the architecture of the University network and/or its technology resources;
 - the most recently tested and approved software patches available;
 - the most contemporary and available security configurations;
 - the most contemporary and available malware protection;
5. Collect appropriate information regarding devices compromised by electronic security incidents. Disconnect affected information technology devices from the network, where appropriate.
6. Follow electronic security incident reporting requirements in accordance with University Policy, Reporting Electronic Security Incidents.

◆ Note: Local system providers should be mindful of potential responsibilities they may also have as custodians of administrative data transmitted or stored on IT devices under their control.

Obligations of the Unit Information System Security Liaison (ISSL) Person(s)

The unit security person(s)/liaison is the person whom the unit head designates as the primary contact for the IT Security Officer and is responsible for performing unit or system IT security. For further guidance or clarification, contact the IT Security Officer.

The unit security person(s)/liaison is responsible to do the following:

1. Act as the unit point of contact with UNLV IT Information Security Officer.
2. Implement a security program consistent with the requirements of this policy and related policies consistent with university guidelines and practices and in keeping with the specific information communication privacy and security needs of his or her unit. This will include overseeing unit compliance with relevant information technology privacy and security regulations under federal, state, and local law, and NSHE and UNLV policy, and will include the following:
 - a. Identify the information technology resources under his or her control.
 - b. Oversee compliance with all information technology security regulations under federal, state, and local law.
 - c. Provide proper information and documentation about those resources.
 - d. Participate in and support security risk assessments of his or her information technology resources, including:
 - the degree of sensitivity or importance of the data transmitted or stored on those resources;

- the criticality of its connection to the network and a continuity plan in the event that it must be disconnected or blocked for security reasons;
 - the vulnerability of a particular resource to be used for illegal or destructive acts;
 - the recovery plan to be followed in the event of disaster;
 - the measures routinely taken to ensure security for each device.
3. Act as the security coordinator for the local support provider(s) within his or her unit (in units where the unit security liaison is not the local support provider).
 4. Participate and assist the IT Information Security Officer, or designated representative, in conducting authorized investigations within their unit.
 5. Take appropriate actions to eliminate problem sources of traffic from the UNLV network, up to and including blocking the information technology device.
 6. Initiate escalation procedures, such as notification of the IT Security Officer, Unit Head, the UNLV Campus Police, or the Student Judicial Affairs Office as necessary.
 7. Implement unit procedures and protocols for the reporting of electronic security incidents in accordance with University Policy, Reporting Electronic Security Incidents including:
 - a. Open and maintain problem reports for electronic security incidents.
 - b. Contact users of and/or local support providers for compromised devices.
 - c. Communicate to local support providers and users, any actions that need to be taken, the reasons for them, the steps required to reestablish service, and any relevant technical information about the incident.

◆ Note: The Unit Security Liaison may want to take specific measures toward the protection of data stored or transmitted on the IT devices under his or her management and/or be mindful of any potential responsibilities as custodians of administrative data.

Obligations of the Unit Head

Unit heads or individuals with responsibility for administrative units have overall, local responsibility for the security of information technology resources under their control. For further guidance, contact your Unit Security Person(s)/Liaison or the UNLV IT Security Officer.

The unit head's oversight responsibilities in relation to security information technology resources include, but are not limited to, the following:

1. Identify a Unit Security person(s)/Liaison to the IT Security Officer, who may in some cases also be the local system provider (depending upon the size of the unit and discretion of the unit head).
2. Ensure that, through the Unit Security Person/Liaison, a security program is implemented for the unit consistent with requirements of this policy (for example, the implementation of security assessment, best practices, education and training), consistent with university guidelines and practices and in keeping with the specific information technology security needs of his or her unit.

3. Provide administrative control over continuity of support over all the IT devices in the unit such that, for example, a change in employment of an individual local support provider does not result in the abandonment of responsibility over IT devices attached to the network.
4. Oversee the creation and implementation of procedures for the reporting of electronic security incidents in accordance with University policy - Reporting Electronic Security Incidents.
5. Assume final responsibility for the security of information technology devices within his or her group or unit.
6. Complying with the obligations delineated under "the User" subsection above.

◆ Note: Unit heads may want to take specific measures toward the protection of data stored or transmitted on the IT devices under their management. Please consult with University policies on data stewardship and custodianship, for further guidance.

Obligations of the UNLV Information Security Officer

The UNLV IT Security Officer is the University officer with the authority to coordinate campus information technology security and related investigations.

The obligations of the UNLV IT Security Officer are to:

1. Oversee, assist or lead electronic or security incident investigation and resolution for the University and individual units. Use approved computer forensic methodologies as required.
2. Ensure proper identification, analysis, resolution, and reporting of UNLV digital security incidents.
3. Oversee and support authorized university-level electronic monitoring and analysis.
4. Support and verify electronic communication privacy and security compliance with federal, state, and local legislation.
5. All digital investigations must follow the authorization procedures outlined below.
6. Conduct/oversee IT security audits.