

Information Technology Policy Manual
with References to Related Procedures and Guidelines

University of Nevada, Reno

Information Technology

June 2007

Table of Contents

1. Introduction.....	2
2. Levels of Information Technology Security.....	4
3. Information Security Participation.....	5
4. Different Types of Digital Information.....	6
5. Access to Information Technology and Data Resources.....	7
6. Protection of Data and Information.....	12
7. Passwords.....	15
8. Acquisition/Disposal of Information Technology Equipment and Media.....	16
9. Security Incidents.....	17

1. Introduction

1.1. Purpose

- 1.1.1. In support of its educational, research, and service missions, the University of Nevada, Reno relies heavily on information technology
- 1.1.2. The University acquires, develops, and maintains computers, computer systems, and networks to provide access to data and information essential to the operation of the University
- 1.1.3. While far from comprehensive, the following compilation of information technology security policies is a tool in an effort to assure the availability, integrity, and appropriate confidentiality of University information resources

1.2. Objectives

- 1.2.1. The primary objectives of the policy documents are development and implementation of measures to prevent security problems and to provide guidance in response to security incidents when prevention is defeated
- 1.2.2. The topics as well as the format of this document loosely follow ISO17799, the preeminent international generic security standard, representing best practices in information systems security
- 1.2.3. By its very nature, policies and procedures related to information technology are dynamic
- 1.2.4. Continuous review of existing policies takes place

1.3. Policy Context

- 1.3.1. The basis for much of the University's information policy is a result of numerous federal and state laws and administrative regulations related to the protection of data. Among them are:
 - 1.3.1.1. The Family Educational Rights and Privacy Act of 1974, (FERPA)
 - 1.3.1.1.1. Commonly referred to as the Buckley Amendment
 - 1.3.1.1.2. Protects the rights of students by controlling creation, maintenance, and access of educational records
 - 1.3.1.1.3. Guarantees students' access to their academic records
 - 1.3.1.1.4. Prohibits unauthorized access by others
 - 1.3.1.2. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
 - 1.3.1.2.1. Includes significant privacy requirements by creating national standards to protect personal health information
 - 1.3.1.3. Gramm-Leach-Bliley Act (GLBA)
 - 1.3.1.3.1. Targeted financial institutions
 - 1.3.1.3.2. Requires universities to maintain an information security program for the protection of financial information
 - 1.3.1.4. Payment Card Industry (PCI) Data Security Requirements
 - 1.3.1.4.1. Applies to all members, merchants, and service providers that capture, store, process, or transmit credit card data

1.4. Policy Development

- 1.4.1. General information technology policy is found implicitly in
 - 1.4.1.1. University of Nevada, Reno Information Technology Division's Strategic Plan
 - 1.4.1.2. University's statements and actions
 - 1.4.1.3. UNR's Acceptable Use Policy

- 1.4.1.4. Relevant NSHE policy documents
- 1.4.2. Specific information technology policies are developed, adopted, promulgated, and maintained for the benefit and general well-being of the University community
- 1.4.3. Generally, a need is first recognized for a formal information technology policy document or written procedure within the Information Technology Division
- 1.4.4. New policy may be the result of new technologies, new laws and regulations, frequent questions regarding given practices, or concern over appropriate response to a situation
- 1.4.5. Any member of the University community is encouraged to submit topics for policy clarification
- 1.4.6. Drafts of IT policy and procedure documents generally originate from the administrative offices of the Vice President for Information Technology
- 1.4.7. Depending on the nature of the policy, the draft may be submitted to the Faculty Senate Information Technology Committee, university officers in affected divisions, legal counsel, and/or the President's Council as a whole
- 1.4.8. Most policies reflect
 - 1.4.8.1. Requirements of practice as outlined in statute or regulations
 - 1.4.8.2. Industry best practices, modified to fit within a university setting
- 1.4.9. If, in the opinion of the Vice President for Information Technology, the proposed policy requires greater debate, s/he may seek the advice of any/all of the above-named bodies or individuals
 - 1.4.9.1. Policies developed following this track will be submitted to the President's Council for final approval
- 1.4.10. Most information technology policies are initially promulgated as policy bulletins that are later codified into the Information Technology's Policy document
- 1.5. Parameters of digital information security at the University of Nevada, Reno
 - 1.5.1. University of Nevada, Reno campus information security for centrally managed resources is
 - 1.5.1.1. Coordinated amongst all groups
 - 1.5.1.2. Controlled appropriately
 - 1.5.1.3. Audited periodically
 - 1.5.1.4. Improved regularly
- 1.6. Campus information policy assumptions
 - 1.6.1. Regardless of security level, campus resources are not assured of appropriate security unless all resources are secure
 - 1.6.2. One should never assume that any computing environment is entirely secure
 - 1.6.3. Regular security audits and network probes help identify weak points
- 1.7. Implications
 - 1.7.1. Management support throughout the campus community is required to maintain an acceptable level of campus information security
 - 1.7.2. Under the central authority of the University of Nevada, Reno campus Information Technology Division, departmental security practices and those

charged with carrying out security in those departments must cooperate on security issues

- 1.7.3. Specific information, security responsibilities, and authorities are articulated across the campus to ensure preemptory activity as well as the ability to provide prompt responses to security problems
- 1.7.4. Periodic audits of server, network, and file security are conducted across the University of Nevada, Reno's infrastructure

2. Levels of Information Technology Security

- 2.1. Different levels of information security and various contractual agreements require the Information Technology Division to support many types of information and diverse users
- 2.2. The University of Nevada, Reno handles many types of information:
 - 2.2.1. Information that is critical to the primary operational missions of instruction, research, and outreach
 - 2.2.2. Confidential information, such as selected personnel data, student demographic data, student academic information, and protected intellectual property related to research on campus
 - 2.2.3. Information, such as personal databases and routine email on desktop computers, which may not require elaborate protection on the part of central Information Technology
- 2.3. UNR Users
 - 2.3.1. Students (Graduate, Undergraduate, Non-degree Seekers)
 - 2.3.2. Classified Staff
 - 2.3.3. Academic Faculty
 - 2.3.4. Research Faculty
 - 2.3.5. Administrative Faculty
 - 2.3.6. Administration
 - 2.3.6.1. Each of the above user groups may have various sub-groups
 - 2.3.6.2. Information security and access issues may differ for each type of information and user
 - 2.3.6.3. Different users within any of these groups may have unique end user access requirements
 - 2.3.7. Implications of multi-level security
 - 2.3.7.1. Information and data needs for each user group requires general definition with associated access privileges
 - 2.3.7.2. Definition of security classes by data type (e.g., sensitive, confidential, public) and appropriate levels of access are defined at the user level, depending on end user requirements and needs
 - 2.3.7.3. To assure sufficient flexibility for the University to accomplish its goals, access services and restrictions can apply to user type, data, information, or services
 - 2.3.7.4. User security profiles often reflect a combination of all of these factors
 - 2.3.7.5. Different types of users require different degrees of authorization to obtain appropriate levels of access to data, information, and services

2.3.7.6. Access privileges may be obtained by application via department heads to Information Technology

3. Information Security Participation

3.1. Assumptions

- 3.1.1. All members of the University community need to be active participants in practicing information security
- 3.1.2. All employees should handle all information and information technology resources in a manner that does not compromise the University's information security
- 3.1.3. Information technology staff have a special responsibility in demonstrating and explaining best security practices to University computer users

3.2. Employee/Manager Implications

- 3.2.1. All employees should exercise sound judgment to maintain, protect, and responsibly share information and data
- 3.2.2. Employees should never share student and human resources administrative information and data with individuals outside their immediate organization without prior authorization
- 3.2.3. Department managers are responsible for their staff's appropriate use of the University's computers and related services
- 3.2.4. Failure to comply with computer security and privacy policies can be grounds for disciplinary action
- 3.2.5. Employees should avoid storing University protected administrative information on personally owned computers without prior authorization of their department head
- 3.2.6. If University confidential or sensitive information is received and/or even briefly maintained on personally owned computer devices (which can include an increasingly diverse array of devices), the employee is responsible for protecting and disposing appropriately of the data and/or information

3.3. Data and Software Implications

- 3.3.1. Each department and division is responsible for insuring that data on desktop computers is backed up regularly
- 3.3.2. In most instances, backup of any critical information can be delegated to campus Information Technology
- 3.3.3. Information Technology maintains a central, comprehensive, tested backup procedure that includes making backups, storing backup material, and recovering data. Unless departments' information and data is included in Information Technology's backup process, the responsible unit must maintain best practices-based backups
- 3.3.4. From the perspective of University policy, there is a presumption of privacy in the files (including email) that may reside on an employee's computer
 - 3.3.4.1. Such files may be deemed state property under current *Nevada Revised Statutes*
 - 3.3.4.2. Personal files on University computing equipment may be determined, at some future time, to be a state record

- 3.3.4.3. Files can be searched for litigation purposes with an appropriately served subpoena
- 3.3.5. Personally owned software should not be placed on a University computer without prior authorization
- 3.4. Benefits, Risks, and Costs of Digital Information Security
 - 3.4.1. Information security requires University resources
 - 3.4.2. Not all institutional information that resides on employees' computers are of equal value, importance, or in need of the same level of security protocols
 - 3.4.3. Information security measures are regularly balanced against the risks and benefits involved
- 3.5. Assumptions
 - 3.5.1. Security measures generally have financial impacts, require personnel time, and inconvenience users and administrators of services
 - 3.5.2. Data and information must be protected as required by state and federal statute and regulations as well as by policies of the Nevada System of Higher Education
- 3.6. Cost implications include:
 - 3.6.1. Extra routers to cope with more dynamic filtering capabilities
 - 3.6.2. Expansion of firewall security
 - 3.6.3. Operational costs, including personnel
 - 3.6.4. Costs in convenience, productivity, and staff morale

4. Different Types of Digital Information

- 4.1. The University of Nevada, Reno's digital information can generally be categorized into three types:
 - 4.1.1. Critical and Sensitive
 - 4.1.1.1. Broadly defined, critical and sensitive data and information is vital to the mission and function of the University
 - 4.1.1.2. Loss of this data would have an unacceptable impact of daily operations and the University's ability to fulfill its mission
 - 4.1.1.3. Such records include, but are not limited to:
 - 4.1.1.3.1. Financial and accounting records,
 - 4.1.1.3.2. Salaries
 - 4.1.1.3.3. Budget records
 - 4.1.1.3.4. Privileged legal Information
 - 4.1.1.3.5. Security procedures, operations, and processes
 - 4.1.1.3.6. Operational vulnerability assessments
 - 4.1.1.3.7. Police records
 - 4.1.1.3.8. Critical infrastructure design and operations
 - 4.1.1.3.9. Ongoing vendor and supplier negotiations
 - 4.1.1.3.10. Security investigations and related information
 - 4.1.1.3.11. Passwords, security control codes, access codes, and security mechanisms for systems, networks, and applications
 - 4.1.1.3.12. Draft financial information and analysis that is being used for internal deliberations and which has not been officially certified and submitted for public release

- 4.1.1.3.13. Intellectual property licensed for the exclusive use of the University community or portions of the University community
 - 4.1.1.3.14. Intellectual property information prior to registration
 - 4.1.1.3.15. Certain sponsored project information protected by statute
 - 4.1.2. Confidential
 - 4.1.2.1. Data stores deemed confidential consist primarily of:
 - 4.1.2.1.1. Student records, including all instances of academic history
 - 4.1.2.1.2. Online coursework
 - 4.1.2.1.3. Financial aid records
 - 4.1.2.1.4. Human resources and personnel records
 - 4.1.2.1.5. Payroll, benefits, and health plan data and actions
 - 4.1.2.1.6. Clinic patient information
 - 4.1.2.1.7. Privileged legal information
 - 4.1.3. Public information
- 4.2. Formats of information/data
- 4.2.1. University information may be presented or stored in many formats, including but not limited to
 - 4.2.1.1. Paper documents
 - 4.2.1.2. Information on electronic storage media
 - 4.2.1.3. Voice
 - 4.2.1.4. Charts and graphic presentations
 - 4.2.1.5. Audio and video tapes
 - 4.2.1.6. Email
 - 4.2.2. Regardless of format, such information/data must be protected
- 4.3. Scope
- 4.3.1. This policy applies to all members of the University of Nevada, Reno community
- 4.4. Responsibilities
- 4.4.1. Every University employee bears some responsibility for safeguarding protected information
 - 4.4.2. Departmental management personnel are responsible for implementing local information procedures and for monitoring compliance within their respective organizations
 - 4.4.3. The Vice President for Information Technology is responsible for establishing and implementing organization-wide information systems and network security policies, standards, and procedures

5. Access to Information Technology and Resources

- 5.1. Variety of information resources
 - 5.1.1. The University of Nevada, Reno provides access to a wide variety of information and information technology resources to facilitate the educational enterprise of the institution
 - 5.1.2. Many resources are available to all members of the University community
 - 5.1.3. Selected information and information technological resources have a more limited function and are protected under requirements of U.S. federal or state government statutes or Nevada System of Higher Education policies

- 5.2. Access to resources varies based on the status of the individual in the institution as well as the intended use of the information
- 5.3. Public higher education's task in handling information resources and accompanying technology is complex
 - 5.3.1. Higher education generally desires to provide the broadest possible access to its information resources and provide maximum transparency of its activities
 - 5.3.2. Conversely, higher education institutions are being required to provide high levels of security for its systems to ensure the integrity of its operational data and to reduce exposure to unauthorized access to critical and confidential data and information
- 5.4. Assumptions
 - 5.4.1. Almost every member of the University of Nevada, Reno community relies on information and information technology to perform their job functions and to support the institution's mission
 - 5.4.2. Access to information resources should be as simple as possible while maintaining assurances of data accuracy, integrity, and confidentiality, as appropriate
 - 5.4.3. Information security measures may occasionally complicate legitimate information access
 - 5.4.3.1. The consequences of security problems that result in unauthorized access can be severe and include
 - 5.4.3.1.1. Time, effort, and monetary resources to correct security problems and notify all affected
 - 5.4.3.1.2. Damage, deletion, and compromise of critical data and information
 - 5.4.3.1.3. Damage to institutional reputation
- 5.5. Unit Responsibilities
 - 5.5.1. Managerial staff is responsible for determining when the user accounts of ex-employees can be removed from the system and destroyed
 - 5.5.2. Managerial staff is also responsible for notifying the correct personnel to carry out such actions
 - 5.5.3. Employees should exercise precautions when sending or receiving information over the Internet to prevent viruses, worms, Trojan horses, and other potentially damaging software
 - 5.5.4. Employees should be aware that while computer files that reside on their desktop computer receive the presumption of privacy, such privacy cannot be guaranteed under a number of circumstances outlined elsewhere in this policy
 - 5.5.5. All members of the University community must respect and adhere to all copyrights and licensing agreements
 - 5.5.5.1. Primary responsibility for enforcing the terms of software agreements and preventing illicit software copying reside at the local departmental level
 - 5.5.5.2. Guidance in the appropriate observance of such agreements is available from the Information Technology Division

5.6. Infrastructure Security Implications

- 5.6.1. Guidelines for remote access to campus information resources follow standard protocols to reduce risk
- 5.6.2. Dial-in modems must not be left on auto-answer when connected to University of Nevada servers or desktop computers
 - 5.6.2.1. Exceptions to this policy provision must be reviewed and approved by the Vice President for Information Technology who will issue guidelines for potential exceptions and the circumstances that warrant them
- 5.6.3. Access to information and resources from remote locations and systems should be available only via strong password provision
- 5.6.4. Connections between computers attached to the University of Nevada, Reno campus network and computers outside the University of Nevada, Reno's network must adhere to the University's firewall design
- 5.6.5. Former University of Nevada, Reno employees should not have access to any systems that might provide access to restricted administrative information
 - 5.6.5.1. With the exception of emeritus faculty, access to University systems should be removed immediately prior to the termination of work by an employee for the institution
- 5.6.6. If managers wish to provide for alternative access to maintain business activities during leaves of absence, provision should be made by means other than sharing passwords
 - 5.6.6.1. For assistance in this matter, contact UNR Campus Information Systems

5.7. Computer Security Implications

- 5.7.1. Password security must be implemented and enforced
- 5.7.2. Department managers are responsible for assuring that passwords for ex-employee accounts are changed promptly by sending an e-mail to Information Technology
- 5.7.3. Employees who will be leaving the University should be asked to remove any email that may not have direct relevance to their job prior to the end of their employment
- 5.7.4. Provision should be made to the account to provide an automatic notification of suspension of the account to any sender of email
 - 5.7.4.1. Directions in the notification, sent via return mail, should provide the sender with information regarding who is assuming the departed employee's responsibilities
- 5.7.5. Account, file, and device access privileges, including file sharing on desktop computers, should not be turned on by default
- 5.7.6. Guidelines, in all instances, exist to determine who has access to given computers on campus, how the decision is made, and how administrative account usage is monitored and logged

5.8. Physical Security Implications

- 5.8.1. Physical security for computer rooms and public computer areas must be observed

- 5.8.1.1. Biometric, restricted key, or electronic card key access must be enforced for all computer rooms and network access points
- 5.8.1.2. Sensitive and/or confidential record information must be secured
- 5.8.1.3. Printed copies, disks, tapes, and other storage devices should be kept in locked cabinets or rooms
- 5.8.1.4. When no longer needed, confidential and/or sensitive hard copy output should not be recycled
- 5.9. Guidelines related to access to University accounts
 - 5.9.1. Information technology support personnel shall provide access or permit access to individual accounts, if he or she
 - 5.9.1.1. Has written (verifiable email or paper) permission from the individual to whom the account or device has been assigned; or
 - 5.9.1.2. In an emergency situation, has a reasonable belief that a process active in the account or on the device is causing or will cause significant system or network degradation, or could result in loss/damage to system or other users' data
 - 5.9.1.3. Information technology support personnel shall provide access or permit access to individual accounts, after consultation with the Vice President for Information Technology, if he or she
 - 5.9.1.3.1. Receives a written authorization from the University President for situations where there is reasonable belief that the individual to whom the account or device is assigned or owned has perpetrated or is involved in illegal activities using the accounts or device in question
 - 5.9.1.3.2. Receives a written authorization from the President for situations where there is reasonable belief that the individual to whom the account or device is assigned or owned has perpetrated or is involved in serious violation of University policy using the accounts or device in question
 - 5.9.1.3.3. Receives a written request from the senior executive officer of a department to access the account of a staff or faculty member who is deceased, terminated, or is otherwise incapacitated or unavailable, for the purposes of retrieving material critical to the operation of the department
 - 5.9.1.3.4. Receives a written request from the Vice President of Student Services on behalf of the parents or estate manager of a deceased student
 - 5.9.1.3.5. Receives a written authorization from the Vice President of Student Services for situations where there is reasonable belief that a student to whom the account or device is assigned or owned has perpetrated or is involved in illegal activities using the accounts or device in question
 - 5.9.1.3.6. Receives a written authorization from the Vice President for Student Services for situations where there is reasonable belief that a student to whom the account or device is assigned or owned

- has perpetrated or is involved in serious violations of University policy using the accounts or device in question
- 5.9.1.3.7. Receives a legal court order and subsequent direction from University Counsel
- 5.9.1.3.8. Receives other legal documents and subsequent direction from University Counsel
- 5.9.2. Preservation of University Account Information by IT
 - 5.9.2.1. If University officials are notified of a University or law enforcement investigation for alleged misconduct or illegal activity on the part of a member of the University community, the contents of an individual's e-mail, other computer accounts, office computer, or network traffic may be copied and stored to prevent destruction and loss of information, pending formal review of that material
- 5.9.3. Subsequent release of the stored materials must be in accordance with the above-specified criteria
- 5.9.4. Except when inappropriate or impractical, all efforts will be made to notify the involved individual prior to accessing a computer account or device, or before observing network traffic attributed to them
 - 5.9.4.1. Where prior notification is not appropriate or possible, all efforts will be made to notify the involved individual as soon after the access as is possible
- 5.10. System-generated, content-neutral information ("metadata") may be used for the purposes of monitoring system and storage utilization, problem troubleshooting, security administration, technology abuse or misuse incident investigation, and in support of formal audits
 - 5.10.1. This information includes
 - 5.10.1.1. Operating system logs (i.e., record of actions or events related to the operation of the system or device)
 - 5.10.1.2. User login records (i.e., what usernames were used to connect to University systems, from where, and when)
 - 5.10.1.3. Network activity logs (i.e., what connections were attempted or completed to University of Nevada, Reno systems, from where, and when)
 - 5.10.1.4. Email logs (i.e., who sent email to or from University of Nevada, Reno email systems, and when)
 - 5.10.1.5. Auditing logs (i.e., records of what actions were taken on University of Nevada, Reno systems, against what resources or applications, and when)
- 5.11. Any intrusive or restrictive University actions related to information technologies will be in accordance with guidelines and procedures set forth in applicable NSHE or University policies, codes, bylaws, or federal or state statute
 - 5.11.1. Such laws include (but are not limited to)
 - 5.11.1.1. The Health Information Portability and Protection Act (patient medical information)
 - 5.11.1.2. Family Educational Rights and Privacy Act (student records)
 - 5.11.1.3. Electronic Communication Privacy Act

- 5.11.1.4. No Electronic Theft Act
- 5.11.1.5. The Digital Millennium Copyright Act
- 5.12. General Procedural Reference
 - 5.12.1. Where reasonably possible and feasible, IT technical support personnel receiving requests for access to computer accounts, files, or network traffic logs by persons other than the account holder will contact the Vice President for Information Technology prior to granting access
 - 5.12.2. The Vice President will provide oversight to ensure that the provisions of this policy have been followed
 - 5.12.3. Where prior consultation is not possible, the Vice President for Information Technology or her/his designated representative will be informed as soon as possible after access is granted
- 5.13. Court orders and other legal documents
 - 5.13.1. Legal documents directing that access be afforded to law enforcement agencies should be delivered to University of Nevada, Reno's University Counsel
 - 5.13.2. Should such documents be served on individual IT support staff or other persons, the document should immediately be delivered to University Counsel for review
 - 5.13.3. After reviewing the order, University Counsel will pass the request and any pertinent advice or instructions to the Vice President for Information Technology

6. Protection of Data and Information

- 6.1. Definition
 - 6.1.1. A computer is defined as any system, server, workstation, PDA, cell phone, etc. that runs an operating system
- 6.2. Critical or confidential information stored on such devices should be protected from disclosure to, modification of, or theft by unauthorized persons
 - 6.2.1. Controls should be in place to minimize loss or damage
- 6.3. General Guidelines
 - 6.3.1. Users should not store, long-term, critical or confidential University information on personal computers
 - 6.3.1.1. File servers should be used to store such information since appropriate access restriction can be applied for such data
 - 6.3.1.2. Accuracy of information is also ensured by regular backup at the server level
 - 6.3.2. Employees must not make unauthorized copies of University-owned or others licensed software or products
 - 6.3.3. Sensitive or confidential information, when printed, should be cleared from printers immediately
 - 6.3.4. The following control measures should be undertaken by users to secure their personal computers from unauthorized access:
 - 6.3.4.1. Users should terminate or lock their logon session if they are leaving the desktops unattended

- 6.3.4.2. Best practice is to have one's machine automatically logoff after a brief period of inactivity
- 6.3.4.3. Hard disk(s) and other storage media on personal computers should not be shared
 - 6.3.4.3.1. In the event sharing is required, media should be shared via an access control list with no open shares (Everyone with either READ or higher access)
- 6.3.4.4. Employees must protect workstations and company networks from computer viruses by using virus scanning applications provided by the University of Nevada, Reno Information Technology
 - 6.3.4.4.1. It is the responsibility of each employee to ensure that the virus scanning software on individual workstations be maintained with the latest updates
 - 6.3.4.4.2. Do not disable or modify this software
- 6.4. Facility/Physical Protection
 - 6.4.1. University of Nevada, Reno facilities must be secure and access must be restricted to areas where confidential information is processed, used, and stored
 - 6.4.2. Centralized computer facilities that house core data will be protected in a physically secure location with controlled access
 - 6.4.3. Computer facilities that process departmental data may require physical security depending on the value and sensitivity of the data they process, the resources they access, and their cost
 - 6.4.3.1. This security is the responsibility of the department
- 6.5. Personally-owned PCs
 - 6.5.1. The usage of personally-owned PCs or laptops by University employees conducting official University business is not generally permitted
- 6.6. Viruses, Worms, Trojan Horses, and Combination Threats
 - 6.6.1. The University of Nevada, Reno's network and computers are routinely monitored for potential break-ins and security breaches
 - 6.6.2. Information Technology maintains and reviews a central log of all security issues
 - 6.6.3. All computers must run current anti-virus software
- 6.7. Spam and Virus Filters (Network)
 - 6.7.1. University of Nevada, Reno's Information Technology Division addresses the problem on a multilevel basis
 - 6.7.1.1. Central management online
 - 6.7.1.2. Client-side solutions
 - 6.7.1.2.1. Faculty and staff can modify their preferences to decrease the amount of spam delivered to email inboxes
 - 6.7.2. The Information Technology Division will provide end user access to all email (albeit in alternative files) directly addressed to them
- 6.8. Laptop and Mobile Device Protection
 - 6.8.1. Increased use of a wide variety of mobile computing and storage devices (Personal Digital Assistants, Blackberry devices, MS SmartPhones, next

- generation cell phones, etc.) present heightened digital information security risks
- 6.8.1.1. Small size (easily misplaced or lost)
- 6.8.1.2. Weak or non-existent user authentication
- 6.8.1.3. Ease by which devices interconnect with other devices and networks
- 6.9. Maintaining copies of files of critical and confidential data/information on a portable device is not encouraged
 - 6.9.1. If critical or sensitive information is stored on a mobile device, password protection and, whenever possible, encryption should be used
- 6.10. A stolen/lost laptop represents two security incidents
 - 6.10.1.1. The computer and potential network access
 - 6.10.1.2. Information/data stored on the computer
- 6.11. Precautions
 - 6.11.1. A device should display generic return information, or be labeled with return information
 - 6.11.2. Do not leave devices unsecured outside of one's office
 - 6.11.3. Do not leave devices unattended in open view in one's hotel room
 - 6.11.4. Do not leave devices unattended and in open view in one's automobile
 - 6.11.4.1. If one must leave it in an automobile, lock the device in the trunk
 - 6.11.5. Never place the device in checked baggage
 - 6.11.6. Keep the device securely with your person in hotel lobbies, airports, restaurants, and other public places
- 6.12. Reporting stolen/lost laptops/devices
 - 6.12.1. Misplaced or stolen devices should be reported to Information Technology immediately
 - 6.12.1.1. Some devices can be remotely locked and/or have its data deleted by IT
- 6.13. Backup and Restoration of Data
 - 6.13.1. Campus IT directly performs or facilitates backup services for all University units requiring backup assistance
 - 6.13.1.1. Secure offsite storage facilities that provide courier service
 - 6.13.1.1.1. Present, principal offsite facility is operated by Iron Mountain, Sacramento, CA
 - 6.13.1.1.2. Service is available to all departments on campus by contacting Information Technology
 - 6.13.2. Systems and data housed in Information Technology's major server facilities
 - 6.13.2.1. Maintained following industry-standard best practices
 - 6.13.2.2. Performed according to a schedule defined by IT's system administrators responsible for administrative and academic mission critical systems

Passwords

7. This policy applies to all University of Nevada computer “Users” as well as to anyone who uses, possesses, or has access to University communications systems
 - 7.1. Common uses of passwords include
 - 7.1.1. User level accounts
 - 7.1.2. Web accounts
 - 7.1.3. Email accounts
 - 7.1.4. Screen saver protection
 - 7.1.5. Voicemail
 - 7.2. General Guidelines
 - 7.2.1. All user-level passwords (e.g., email, desktop computer, local/domain, etc.) must be changed at least every 365 days [projected implementation 2008]
 - 7.2.2. Passwords must not be inserted into email messages or other forms of electronic communication
 - 7.2.3. All user-level and system-level passwords must conform to the guidelines described below
 - 7.2.3.1. A standard, default password should not to be granted for all users or groups of users
 - 7.3. Password strength
 - 7.3.1. Members of the University community must be aware of the importance of maintaining strict, confidential ownership of strong passwords
 - 7.3.1.1. Characteristics of strong passwords
 - 7.3.1.1.1. Contain both upper and lower case characters (e.g., a-z, A-Z)
 - 7.3.1.1.2. Contain numbers (0-9)
 - 7.3.1.1.3. Contain at least six characters
 - 7.3.1.1.4. Is not a word in any language, slang, dialect, jargon, etc.
 - 7.3.1.1.5. Are not based on personal information, names of family, etc.
 - 7.3.2. Weak passwords, which commonly have the following characteristics, will not be permitted on University of Nevada, Reno systems
 - 7.3.3. Characteristics of weak passwords
 - 7.3.3.1. A password containing fewer than six (6) characters
 - 7.3.3.2. A password consisting of a word found in any language (English, non-English, slang, jargon, proper nouns, etc.)
 - 7.3.3.3. Password in common usage, such as:
 - 7.3.3.3.1. Names of family members, pets, friends, co-workers, fantasy characters, etc.
 - 7.3.3.3.2. Computer terms and names, commands, sites, companies, hardware, software
 - 7.3.3.3.3. Birthdays and other personal information such as addresses and phone numbers
 - 7.3.3.3.4. Word or number patterns like aabbccdd, qwerty, zyxwvuts, 12344321, etc.
 - 7.3.3.3.5. Any of the above spelled backwards
 - 7.3.3.3.6. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

- 7.3.3.3.7. Any of the above with some letters substituted (i.e. passw0rd)
- 7.4. Password management
 - 7.4.1. Passwords should never be written down or stored online
 - 7.4.2. Passwords should NEVER BE SHARED WITH ANYONE FOR ANY REASON, including IT support personnel, administrative assistants, or secretaries
 - 7.4.2.1. If such a request is made, contact Information Technology support immediately
 - 7.4.3. University passwords should never be used in any non-University application
 - 7.4.4. All passwords are to be treated as sensitive, confidential information
 - 7.4.5. If an issue or situation arises that requires sharing one's password, change it at the first opportunity
 - 7.4.6. If a member of the staff requires access to another's account (due to prolonged absence, administrative assistant, etc.), assignment of the account should be practiced rather than sharing passwords.
 - 7.4.7. Do not use the "Remember Password" feature of applications (e.g., Microsoft Internet Explorer, Microsoft Outlook, Mozilla Firefox, Netscape Messenger, etc.).
 - 7.4.8. If one suspects an account or password has been compromised, report the incident and change all passwords
- 7.5. Password Testing
 - 7.5.1. IT Security, through various means, may perform password cracking tests on a periodic or random basis
 - 7.5.2. If a password is guessed or cracked during one of these scans, the user will be required to change the password
 - 7.5.3. Account Lockout
 - 7.5.3.1. Many University systems will lock accounts after a pre-set number of consecutive failed login attempts
- 7.6. Application Development Standards
 - 7.6.1. Application developers must ensure that programs contain the following security precautions
 - 7.6.1.1. Support authentication of individual users, not groups
 - 7.6.1.2. Must be encrypted on the screen
 - 7.6.1.3. Should not cache the password in a cookie or any other local media format on the client system
 - 7.6.1.4. Provide for role management, such that one user can take over the functions of another without having to know the other's password
 - 7.6.1.5. Should provide security capabilities for all sensitive data

8. Acquisition/Disposal of Information Technology Equipment and Media

- 8.1. Disposal
 - 8.1.1. University surplus property regulations govern the disposal and/or resale of all University property

- 8.1.2. Any computer hard drive or removable magnetic medium, such as a diskette, magnetic tape, flash memory, etc., which has stored any critical or confidential information, must be electronically “cleaned”
- 8.1.3. Information Technology employs a Department of Defense standard data eradicating process to assure data is unrecoverable prior to the device being discarded
- 8.1.4. Non-erasable media, such as a CD, optical disk, etc. used to hold critical or confidential information must be physically destroyed
- 8.2. Purchase
 - 8.2.1. Requests and/or purchase orders for technology purchases, including hardware, software, and peripherals in excess of \$10,000 must be approved by Information Technology
 - 8.2.1.1. Maintain campus standards
 - 8.2.1.2. Assure interconnectivity
 - 8.2.1.3. Assistance to functional users in determining and defining appropriate technology to meet stated needs
 - 8.2.1.4. Verification of compatibility, configuration, and data storage and security requirement
 - 8.2.1.5. Assist in most effective campus technology infrastructure
 - 8.2.2. IT does not control departmental budget dollars nor authorize departmental expenditure of funds

9. Security Incidents

- 9.1. Purpose
 - 9.1.1. Outlines a standard for escalating, reporting, and resolving information security incidents
- 9.2. Scope
 - 9.2.1. This policy applies to all University of Nevada, Reno computer “Users” as well as individuals who may connect to the University’s network, regardless of device type
- 9.3. Definition
 - 9.3.1. An IT security incident is defined as an event that affects or has the potential to affect the confidentiality, availability, or integrity of University of Nevada, Reno digital information, data, or technologies
 - 9.3.2. Potential security incidents include, but are not limited to
 - 9.3.2.1. Any situation that may pose a serious threat to the University of Nevada, Reno’s IT operational or business processes and potentially impact the University of Nevada, Reno’s ability to continue operations or services
 - 9.3.2.2. Security breaches of University of Nevada, Reno systems, whether or not resulting in the loss of University confidential information, intellectual property, or other sensitive information
 - 9.3.2.3. Serious violation of the University of Nevada, Reno Acceptable Use Policy
 - 9.3.2.4. Significant instances of misuse or misappropriations of computer assets and systems

- 9.3.2.5. Thefts or loss of University computing assets
- 9.3.2.6. Unauthorized release of critical or confidential information
- 9.3.2.7. Situations requiring forensic analysis/investigation of University of Nevada, Reno computing assets
- 9.3.3. Reporting
 - 9.3.3.1. Any unauthorized disclosures or uses of protected information, as well as other potential information security issues should be reported immediately to any member of the Information Technology staff
 - 9.3.3.2. Individual(s) who report an incident or potential IT security incident should do so without fear of retaliation and may elect to remain anonymous
- 9.4. Common Steps Followed in a IT Security Incident
 - 9.4.1. Specific procedures vary depending on the nature of the incident, but all procedures include the following steps:
 - 9.4.2. Discovery
 - 9.4.2.1. When a threat is discovered or reported, it is logged by IT security
 - 9.4.2.2. Appropriate IT staff are alerted
 - 9.4.2.3. IT resources are assessed for vulnerability to the discovered threat
 - 9.4.3. Documentation
 - 9.4.3.1. Documentation of the threat begins and continues until the incident is closed
 - 9.4.3.2. Vulnerabilities or potential vulnerabilities are noted
 - 9.4.4. Notification
 - 9.4.4.1. If a vulnerability is discovered, appropriate individuals are contacted via email or telephone, including the Vice President for Information Technology
 - 9.4.4.1.1. The campus Information Security coordinator(s) will confer on any security matter as soon as possible to identify the potential risks/exposure and potential responses
 - 9.4.4.1.2. University of Nevada, Reno IT security will engage, through the Administrative Offices of the Vice President for Information Technology, legal, internal audit, human resources, and other internal resources, as appropriate, in determining the appropriate course of action
 - 9.4.5. Acknowledgment
 - 9.4.5.1. IT support staff in affected areas should respond to notifications as soon as possible
 - 9.4.5.2. Staff in the affected areas should coordinate a plan of action with the University of Nevada, Reno IT security coordinator
 - 9.4.6. Containment
 - 9.4.6.1. Vulnerable IT resources should attempt to be contained until the vulnerability is mitigated and incident is resolved
 - 9.4.6.2. Priority is given to safeguarding critical and confidential data
 - 9.4.6.3. Preliminary findings should provide early formulation of possible resolution of the incident
 - 9.4.7. Investigation

- 9.4.7.1. Network and server managers must investigate vulnerabilities identified in notifications
- 9.4.7.2. IT workers must research applicable security resources to determine appropriate remediation
- 9.4.7.3. If the incident has resulted in a breach that might have exposed confidential data, University Counsel will be contacted and the University of Nevada, Reno Office of Communications will be updated
- 9.4.8. Resolution
 - 9.4.8.1. Network and server managers and others, including data stakeholders, must implement a resolution to resolve vulnerabilities identified in notifications
 - 9.4.8.2. IT workers should follow unit change management procedures to make software updates
 - 9.4.8.3. Common resolutions to correct a vulnerability include
 - 9.4.8.3.1. Upgrading and patching software and/or operating systems
 - 9.4.8.3.2. Imposition of physical, network, host, user, and/or other access restrictions
 - 9.4.8.3.3. Other resolutions may apply depending on the results of the investigation
- 9.4.9. Closure
 - 9.4.9.1. The Security Officer and appropriate staff will review the incident tracking documentation and close service tickets as appropriate
 - 9.4.9.2. Incident will be reviewed to discover any possible lessons to be learned