



OFFICE OF INFORMATION TECHNOLOGY

CAPSTONE POLICY - IS03

PROTECTION OF PERSONAL NON-PUBLIC INFORMATION (PNPI)

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: EACH JULY SECURITY RESPONSE PRIORITY LEVEL: (NA)

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.

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

## Protection Of Personal Non-Public Information (PNPI)

PAGE 2 of 11

---

*The immutable University of Nevada, Las Vegas (UNLV) information security policy is to secure and protect personal non-public information maintained or transmitted by UNLV against all internal, external, deliberate or accidental threats, releases, or misuses.*

**SCOPE AND APPLICABILITY:** *This Policy applies to all UNLV organizations.* Information is a significant and critical asset of UNLV. The purpose of the PNPI Policy is to expand on the Capstone *IS01 Information Security Policy* and the Capstone *IS02 Information Sensitivity and Classification Policy* to establish requirements for protecting personal, non-public information and notifying individuals whose personal, non-public information may have been disclosed by inappropriate release or computer security breaches.

Personal non-public information is any information that uniquely identifies a person and provides confidential information (e.g., academic, financial, medical records) about that individual. Examples of PNPI include, but are not limited to:

- Social Security Numbers (SSN)
- Credit card or bank account numbers
- Medical or educational records
- Other sensitive, confidential or protected data (e.g., grades used in context with personally identifiable information such as name, address, or other easily traceable identifiers).

PNPI in combination with name and security code or password needed to access the credit card or financial account pose a high risk of identity theft, personal jeopardy, or financial loss to the individual if improperly disclosed. Personal, non-public information does not include published directory information or information that is lawfully made available to the general public from federal, state or local government records.

### Protecting Personal Non-Public Information

NSHE, State, and Federal laws and regulations govern the safeguarding of personal, non-public information (PNPI), such as Social Security Numbers (SSNs). The

- Family Educational Rights and Privacy Act (FERPA) [educational records],
- Gramm-Leach-Bliley Act (GLBA) [financial institution and customer data],
- Health Insurance Portability and Accountability Act (HIPAA) [health information], and
- NSHE Board of Regents Bylaws and codes.

all require those who collect PNPI to follow strict guidelines.

The laws concerning personal-identifiable information have elevated the need for security controls at the data level and no longer to just the network. The goal is now to put multilayered defenses around the nonpublic data by layering technology controls to make sure that you can identify where the information passes across the network, and from whom to whom.

### University Departments Must Act

Information protection involves people, processes and technology. At UNLV, all departments must reduce their reliance on SSNs and use alternative forms of identifying students, employees, and faculty

## Protection Of Personal Non-Public Information (PNPI)

PAGE 3 of 11

---

whenever possible. Further, all University departments should follow good practices in safeguarding all personal non-public information (PNPI).

The first step is for each **department, school, or organization** to re-examine its use of and storage practices regarding all PNPI. Departments should review their processes for using PNPI annually:

- "Why are we acquiring PNPI's?"
- "How are we storing any PNPI we do acquire?"
- "How are we protecting the PNPI's that we acquire?"
- "What can we do to train our faculty and staff in the proper use and management of personal non-public information (PNPI) and other confidential information?"
- "Who has access to PNPI's in our department, and do they still need the access?"

Every employee of every University department must work to help the University meet the requirements imposed by NSHE, FERPA, GLBA, HIPAA and other laws to protect the privacy of personal information in UNLV's care. In addition if you are asked to provide a SSN (either your own, another employee's, a student's, a family member's), challenge the request.

In addition to the *IS01* and *IS02* capstone security policies, the University has developed other supporting IT security policies and Guidelines for Protecting Personal Non-Public Information. In addition to containing general information, the University guidelines offer the following advice:

- Ensure the Privacy of PNPI.
- Encrypt Electronic Transmissions.
- Do Not Store PNPI Locally.
- Ensure PNPI Security When Working from Home or Outside the University.
- Have Computer Systems Audited.

Departments with internal IT support should plan accordingly. Planned IT measures should include data encryption, two-factor authentication of users and closer monitoring of user activity; and increased focus on providing the ability to log and audit user transactions.

**BACKGROUND:** The UNLV Provost's Office administers and maintains the UNLV campus-wide environment to meet the academic, privacy, and administrative needs of the UNLV campus community. The *IS01 Information Security Policy*, this policy (*IS03*) along with other high-level capstone policies and supporting mid-level information security policies directly support UNLV's compliance requirements related to:

- Computer Security Act of 1987,
- Health Insurance Portability and Accounting Act (HIPAA) of 1996,
- Privacy Act of 1974,
- Family Educational Rights and Privacy Act (FERPA) of 1974,
- Financial Services Modernization (Graham-Leach-Bliley) Act of 1999,
- NSHE Board of Regents Bylaws (Title 4, Chapter 1, Section 27 of 2006), and
- other Federal and State of Nevada acts, codes, laws, and regulations.

The UNLV information security policies and structure provide an emphasis on assuring that:

- Confidentiality of information will be assured;
- Integrity of information will be maintained;
- Availability of information for business processes will be maintained;
- Legislative and regulatory requirements will be met;
- Business continuity plans will be developed, maintained and tested;
- All actual or suspected digital information security breaches will be reported to the OIT Information Security Office and will be thoroughly investigated.

**POLICY STANDARDS AND CONTROLS:** See the ANNEX for 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:** Policy compliance and enforcement 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 policy reviews and security audits will be conducted annually or more frequently as required. The UNLV CISO, or appointed designee, will conduct security policy reviews and the security audits.
3. 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 and a level of infraction 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. The level of infraction and recourse to such actions shall be as provided for under the provisions of those instruments.
4. The Policy shall also be enforced with assistance from the UNLV Administrative Code Office, NSHE Board of Regents Bylaws, and the NSHE Legal Counsel.

**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.

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

**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.

**SERIES IS – CAPSTONE POLICIES GROUP (Tier 1)**

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

<i>IS01</i>	<i>Information Security for IT Resources Policy**</i>
<i>IS02</i>	<i>Information Sensitivity and Classification Policy (with Handbook)**</i>
<i>IS03</i>	<i>Personal Non-Public Information Policy**</i>
<i>IS04</i>	<i>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</i>	<i>Acceptable Use of IT Resources Policy (Users)**</i>
<i>101B</i>	<i>Acceptable Use of IT Resources Policy (Mgmt &amp; SysAdmin)**</i>

**SERIES IST400 – IT OPERATIONS & PROVISIONING GROUP (Tier 2)**

Policies that provide for monitoring and logging, provisioning and implementation, assessment and compliance, system administration, remote access, physical security, configuration management, and training and awareness programs.

<i>402</i>	<i>Risk Assessment and Management Policy (with Handbook)**</i>
<i>406</i>	<i>Data Media Sanitization &amp; Destruction Policy (with Guide)**</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***

**Protection Of Personal Non-Public Information (PNPI)**

PAGE 6 of 11

---

- 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

<b>Subject</b>	<b>Contact</b>	<b>Telephone</b>	<b>Email/URL</b>
Policy Clarification	Office of Information Technology	(702) 895-0500	<a href="http://www.UNLV.edu/infotech/policy.html">http://www.UNLV.edu/infotech/policy.html</a>
Legal Issues	Administrative Code Officer	(702) 895-1879	- none -
Information Security	Information Security Officer	(702) 895-5284	<a href="mailto:informationsecurityoffice@unlv.edu">informationsecurityoffice@unlv.edu</a>
Campus Computing Services	Director of Campus Computing Services	(702) 895-0787	- none -
Enterprise Applications Services	Director of Systems & Applications	(702) 895-1765	- none -

---

**DEFINITIONS**

---

Additional definitions of terms as they are used in this policy 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. *Each UNLV administrative department is responsible for development of internal procedures and directives to implement and comply with this policy for their organization.*

**POLICY STANDARD: IS03-1 Required by Law, Code or Policy.** Unless required by law, or needed to perform core departmental activities which cannot be immediately facilitated by other means, Social Security numbers or other high risk personal non-public information must not be collected or stored in unauthorized or unsecured areas or systems.

**POLICY STANDARD: IS03-2 Compliance With Law And Policy.** Campus departments, units, or groups should establish documented security guidelines, standards, or procedures that refine the provisions of this Policy for specific activities under their purview, in conformance with this Policy and other applicable provisions of Federal and state laws that prohibit the theft or abuse of computers and other electronic resources. Two-factor authentication of users should be used including logging of user activity.

**POLICY STANDARD: IS03-3 PNPI Storage.** Personal non-public information should only be stored in approved, locked cabinets or on protected centrally-administered UNLV IT systems. If personal non-public information must be stored locally in the unit on a unit-administered computing system, it must be encrypted and provide the ability to log and audit user transactions.

**POLICY STANDARD: IS03-4 PNPI Encryption.** Secure, encrypted communications shall be used when collecting or transmitting personal non-public information. Personal non-public information should not be sent via e-mail unless required by a government agency. Grades may be e-mailed to a student's official University e-mail address only after receiving the student's explicit permission.

**POLICY STANDARD: IS03-5 PNPI Requirement Re-Evaluation.** University departments must re-evaluate their acquisition, use and safeguarding of personal non-public information for conformance to this policy and University Guidelines for Protecting Personal Non-Public Information at least annually.

**POLICY STANDARD: IS03-6 PNPI Unauthorized Release.** Following the discovery of a breach in the security of a system in which unencrypted high risk personal non-public information may have been accessible or the physical breach and loss/copy of the media, the unit must notify all persons whose personal information might have been acquired by an unauthorized person(s) of the breach of the security of their personal information. A physical security breach is any incident that involves the compromise, loss, or theft of PNPI. A computer security breach is any incident in which the security of a computer system is compromised, including theft or loss of a computer or storage device or medium where unauthorized person(s) might have been able to access, copy or read data files on it. It does not include normal business use by authorized employees or University business partners.

**POLICY STANDARD: IS03-7 PNPI Privacy And Confidentiality.** Technical solutions must be implemented so as to protect the privacy and confidentiality of the various types of electronic or physical PNPI in accordance with all applicable laws and policies. Users who are authorized to obtain data must ensure that it is protected to the extent required by law or policy after they obtain it. For example, when sensitive data is transferred from a well-secured mainframe system to a User's location, adequate security measures equal to the source system must be in place at the destination computer to protect this "downstream data". Additionally, technical staff assigned to ensure the proper functioning and security of University electronic information resources and services are not permitted to search the contents of electronic communications or related transactional information except as provided for in the UNLV Policy. For example, any scanning of network traffic to detect intrusive activities must follow established campus guidelines or organizational procedures to ensure compliance with laws and policies protecting the privacy of the information.

**POLICY STANDARD: IS03-8 Compliance With Security Breach Notification Laws.** Under Nevada Statute 485 effective January 2006, and legal requirements under HIPAA, GLBA, FERPA, and the FTC Safeguards Rule the University is obligated to develop, implement, and maintain an information security program that protects Personal Non-Public Information (PNPI) or personal and student information, and financial information including other information covered by security breach notification laws. To comply with the respective laws and regulations, the University shall establish a security breach notification plan and appoint an office to oversee compliance with applicable security breach notification laws.

**POLICY STANDARD: IS03-9 Compliance With NSHE Board of Regents Data Security Policy.** It is the policy of the Board of Regents, Bylaws Title 4 Chapter 1 Section 27 titled Data Security Policy, that "sensitive data maintained or transmitted by an NSHE institution must be secure. For the purposes of that Section (27), "sensitive data" means any data associated with an individual, including but not limited to social security number and data that is protected by state or federal law." *[See Nevada Senate Bill 347, enacted into law 6.17.2005, for amending the Nevada Revised Statutes Chapter 205, 205.461, 205.4617, 205.463, 205.464, 205.465, 205.4653, and 205.4657, Chapters 52, 597, and 97A, 97A.140, and 97A.293. See also Federal statutes.]*

"Each NSHE institution must develop and maintain policies, standards, and/or procedures that describe and require appropriate steps to protect sensitive data that is maintained on an institution's computing devices or transmitted across a public network such as the Internet. Institutional policies must include the requirements for the eradication of data when computers are sent to surplus or repurposed. Institutions must be aware of all areas that data are stored, both physically and electronically, and must audit these areas annually to ensure that sensitive data are retained or destroyed as appropriate. Each institution must maintain policies and procedures to be followed in the event that sensitive data is released inappropriately."

---

**ANNEX 2 –ROLES AND RESPONSIBILITIES**

---

**Administrative Officials or persons acting in that capacity must:**

- Identify and classify the digital information assets within areas under their control;
- Define the purpose and function of the resources and ensure that requisite education and documentation are provided to the University as needed;
- Establish acceptable levels of security risk for resources by assessing factors such as:
  - How sensitive the data or asset is, such as research or other information protected by law or policy,
  - The level of business criticality or overall importance to the continuing operation of the University as a whole, individual departments, research projects, or other essential activities;
  - How the operations of one or more units would be affected by the loss, unavailability or reduced availability of the assets,
  - How likely it is that an asset could be used as a platform for inappropriate acts towards other devices, persons, or organizations, and
  - Limits of available technology, programmatic needs, cost, and staff support;
- For systems in support of University business administration, ensure compliance with relevant provisions of other UNLV policies;
- Identify and designate a Custodian or "data steward" for the information asset, the authorized University support person or organization responsible for maintaining the safeguards established by Administrative Officials;
- Ensure that requisite security policies, standards, and safeguards are implemented and monitored for the assets;
- It is a University management obligation to ensure that all employees, contractors, students, and volunteers understand and comply with UNLV security policies and standards, as well as all applicable laws and regulations.

*(These are individuals with administrative responsibility for campus organizational units [e.g., control unit heads, deans, department chairs, principal investigators, directors, or managers] or individuals having functional ownership of data or systems)*

**IT Providers/IT Groups or persons acting in that capacity must:**

- Become knowledgeable regarding relevant University security requirements and guidelines;
- Analyze potential threats and the feasibility of various security measures in order to provide recommendations to Administrative Officials;
- Implement approved security measures that mitigate threats, consistent with the level of acceptable risk established by Administrative Officials;
- Establish procedures to ensure that privileged or special accounts are kept to a minimum and that privileged users comply with privileged/special access agreements;
- For systems in support of University business administration, establish procedures to implement relevant provisions of other UNLV policies, such as incident response and recovery;
- Communicate the purpose and appropriate use for the assets under their control.

*(These are the IT class of individuals who design, manage, and operate campus electronic information resources, e.g. project managers, system managers, system designers, application programmers, database administrators (DBA), or system administrators)*

**Users or persons acting in that capacity** must

- Become knowledgeable about relevant University security requirements and guidelines;
- Protect the assets under their control, such as access passwords, computers, and data they download or access.

*(They are individuals who access and use campus electronic information resources)*

Other entities with important campus electronic information resource security responsibilities include **Campus Computing Services, Network Operations Center, Systems and Applications**, and miscellaneous other **Information Technology groups** in various departments, schools, etc.

Insufficient security measures at any level may cause resources to be stolen, damaged, or become a liability to the University. Therefore, responsive actions may be taken. For example, if a situation is deemed serious enough, computer(s) posing a threat will be blocked from network access. (The campus "Guidelines and Procedures for Blocking Network Access" specify how the decision to block is made and the procedures involved.)

---

**GUIDELINES FOR PROTECTING PERSONAL NON-PUBLIC INFORMATION**

---

UNLV Information security efforts are based on the family of University information security policies.

The Board of Regents has established a code (Bylaws Title 4 Chapter 1 Section 27 titled Data Security Policy) whereby "each NSHE institution must develop and maintain policies, standards, and/or procedures that describe and require appropriate steps to protect sensitive data that is maintained on an institution's computing devices or transmitted across a public network such as the Internet." To assist in accomplishing this directive, it is recommended that each UNLV department or organization use the following policies as specific or notional guidelines as appropriate to their operations.

- IS01 Information Security for UNLV IT Resources Policy***
- IS02 Information Sensitivity and Classification Policy***
- IS04 UNLV Infrastructure Responsibilities and Services***
- 101A Acceptable Use of UNLV IT Resources Policy (Users)***
- 101B Acceptable Use of UNLV IT Resources Policy (Mgmt & SysAdmin)***
- 102 Password Standards and Guideline Policy***
- 103 Anti-Virus, Spyware & Malicious Code Policy***
- 104 Reporting Electronic Security Incidents Policy***
- 201 Acceptable E-mail Usage Policy***
- 302 Regulatory IT Compliance Policy (HIPAA, FERPA, GLBA)***
- 303 Remote Access to UNLV Networks and Systems Policy***
- 402 Risk Assessment and Management Policy***
- 403 General Server Security and Access Policy***
- 404 Password Standards for Servers and Network Devices Policy***
- 405 Technical Security of End-Point (User) Systems Policy***
- 408 Computer Security Incident Response for First Responders Policy***
- 501 Technical Security of IT Resources Policy, Standards, & Directives***

"Institutional policies must include the requirements for the eradication of data when computers are sent to surplus or repurposed." See the UNLV information security policy titled:

- 406 Data Media Sanitization & Destruction Policy***

"Institutions must be aware of all areas that data are stored, both physically and electronically, and must audit these areas annually to ensure that sensitive data are retained or destroyed as appropriate." See the UNLV information security policy titled:

- 802 Security Auditing and Vulnerability Scanning Policy***

"Each institution must maintain policies and procedures to be followed in the event that sensitive data is released inappropriately." See the UNLV information security policies titled:

- IS01 Information Security for UNLV IT Resources Policy***
- 104 Reporting Electronic Security Incidents Policy***
- 408 Computer Security Incident Response for First Responders Policy***
- 801 Security Incident Handling and Digital Investigations Policy***