



OFFICE OF INFORMATION TECHNOLOGY

**CAPSTONE
POLICY - IS02**

**INFORMATION SENSITIVITY AND
CLASSIFICATION**

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. This Capstone policy, in concert with Capstone Policy IS01 - *Information Security for Information Resources and Assets* and the other Capstone policies, assists in defining the strategic need and direction for UNLV information security.

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

Information and IT systems are significant assets of UNLV. The University information, excluding third-party intellectual property, includes information that is electronically generated, printed, filmed, typed,

stored, or verbally communicated. All UNLV information assets shall be classified according to its sensitivity, criticality, and value, regardless of the media on which it is stored, the manual or automated systems that process it, or the methods by which it is collected or distributed. Information identified as the property of third-parties that has been entrusted to the University will also be classified and safeguarded in accordance with this and other UNLV policy and in accordance with related agreements.

SCOPE AND APPLICABILITY: This Policy applies to all UNLV organizations and IT systems.

Information is an asset that is critical to the internal operation of the University and may also be governed by Federal and State regulatory statute, and therefore must be protected accordingly. The information covered by the policy include all information collections, both manual and digital, and all IT systems, networks, and facilities administered by individual schools, departments, University laboratories, and other University-based entities.

The principals of confidentiality, integrity, and availability (CIA) must be applied to all University information and the supporting physical assets/systems. To ensure that information assets receive an appropriate level of protection, information must be classified to indicate the need, priorities and degree of protection appropriate.

The University also seeks to safeguard the integrity of UNLV IT assets and data; and to ensure that use of electronic communications complies with the provisions of the Nevada System of Higher Education (NSHE) Code, UNLV Bylaws, and Student Code of Conduct for maintaining public order and the educational environment.

Specifically for IT assets:

1. The Information Security Officer (ISO) is responsible for maintaining the policy and providing the support and advice related to it.
2. All campus IT managers are directly responsible for implementing asset classification on all information and systems in their respective departments or organizations.
3. IT systems will be used for their intended purposes and meet any compliance requirements.
4. The core IT network and systems will be available to support emergency services in the event of community disaster response needs.

BACKGROUND: The University information, excluding third-party intellectual property, includes all information that is electronically generated, printed, filmed, typed, stored, or verbally communicated.

In order to manage information asset security comprehensively, this policy serves four major purposes.

1. It contributes to the overarching or campus-wide information security for the University.
2. It establishes the principle that every information asset must have at least one individual responsible for managing that asset.
3. It establishes the principle that every information technology (IT) device/asset must have at least one individual responsible for managing that device/asset.
4. It establishes the principal that information assets will be managed from a risk management perspective.

and has the following goals:

- to ensure a secure and protective information asset process that promotes the missions of the University in teaching, learning, research, patient care, and administration.
- to ensure a secure and protective IT infrastructure that supports the missions of the University in teaching, learning, research, patient care, and administration, and
- to ensure the academic and business continuity, and to minimize the risk of theft, loss, damage, or misuse of University informational assets by preventing security incidents where possible, detecting and investigating electronic security incidents, and reducing their potential impact.

INFORMATION CLASSIFICATION BASELINE REFERENCE STANDARDS: The UNLV Information Security Policy and its structure is based on *International Standards Organization's ISO 17799/27001 – the International Standard for Information Security*, the Generally Accepted Information Security Principals (GAISP), 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, and the [Federal Information processing Standard \(FIPS\) 199](#) on information security categories.

FIPS 199 establishes security categories for both information and information systems. The security categories are based on the potential impact (low, moderate, high) on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the information-loss risk to an organization. Information is categorized according to its *information type*. An information type is a specific category of information (e.g., Private Non-Public (privacy, medical, or student), proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.

POLICY STANDARDS AND CONTROLS: See the Section below on 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 to administer and maintain this Policy and all related subordinate information security policies. The Policy shall also be maintained and enforced with assistance from the UNLV Administrative Code Office and NSHE Counsel, and NSHE System Computing Services (SCS), and the UNLV Office of Information Technology (OIT). 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 asset 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 IT 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 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 the appropriate parts of BS 7799.2:2002 Audit Check List and through the collective audits of all UNLV information security policies and practices. The UNLV ISO 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)

CONSIDERATIONS

Categories of Assets: Information, Physical, Facility.

When considering the assets to include in the inventory, be sure to identify any supporting IT infrastructure. If an electronic database is a major asset, then the IT server it is sitting on is probably a major asset. The IT backup tapes/storage that come out of it are certainly a major asset. The IT software on which the database runs may or may not be major. Depending on how the database or information are used, (how serious availability is), the IT network routers and cabling may be a major asset even though they may not meet a \$ threshold.

Define handling and labeling requirements to support classifications. – copying procedures/restrictions, storage procedures/restrictions, transmission procedures/restrictions, communication procedures/restrictions, destruction procedures/restrictions.

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 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 & 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 & 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*
- 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
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 -

DEFINITIONS

Additional definitions of terms as they are used in this policy can be found in UNLV document "**Information Security Acronyms, Terms and Definitions**".

Reference Definitions related to assets:

Executive Sponsors: *Those senior University officials who have planning and policy-level responsibility and accountability for data, including creation and maintenance, within their appropriate functional area. They fill a knowledge management role at UNLV. By understanding the planning needs of the institution, they are able to anticipate how data will be needed to meet these needs. The trustees work and bring in people as needed to translate data to accomplish this role*

Data Stewards: *Appointed by Executive Sponsors to carry out the data policies that have been established, as well as the University's overall administrative data security policies.*

Data Administrators: *The authorized University support person or organization responsible for maintaining the safeguards established by the Data Steward(s). The Data Steward designates the Data Administrator. The Data Administrator may be a non-person; that is, a Data Center may be the Data Administrator for the business applications "owned" by a University unit. The Data Administrator may indirectly report to the Data Steward if the person is in another organization but is responsible for supporting the Data Steward.*

User: University employees or persons authorized by the Data Steward to access information and use the safeguards established by the Data Steward.

The roles of UNLV Executive Sponsors, Data Stewards, and Data Administrators are fully defined in the University data policy in the UNLV Office of Institutional Analysis and Planning.

STANDARDS

INFORMATION ASSET SECURITY STANDARDS AND CONTROLS: UNLV's information asset inventory and classification is a set of standards and guidelines that shall be applied to each data collection and IT system/device. Information security efforts based on risk management focus on three principal areas - the sensitivity or classification of data contained in information collections and IT systems, the operational criticality of the processing capabilities of manual and automated information systems, and the security level of those systems. Security Level designations of the information and of the IT systems are used to define the requirements of the integrated security efforts. The first two designations are grouped as Sensitivity and as Criticality, and each designation has multiple levels. (See the Handbook for Information Asset Classification). The asset classification outcome is to be used to establish the appropriate level and cost of information security.

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: IS02-1 Information Classification. All UNLV information collections, data-sets, and databases shall be classified according to its sensitivity and criticality regardless of the media on which it is stored, the manual or automated systems that process it, or the methods by which it is collected or distributed. Data classification shall be accomplished using the Handbook for Information Asset Classification, Part 1 (Steps 1 & 2).

If the collections are automated, information system IT managers are responsible for applying the information classification to the hosting IT systems under their jurisdiction and applying this information to any System Security Plan (SSP) and Risk Assessment initiatives that are required by policy. Each UNLV IT system storing or processing information classified above Unrestricted-Public must have a System Security Plan (SSP). A fundamental component of an SSP that defines information protection requirements is a Risk Assessment. SSPs and Risk Assessments define and evaluate the management controls, operational controls, and technical controls of major applications and general support systems. The UNLV SSP is presented in UNLV policy titled *IT System Security Plans* and UNLV Risk Assessment is presented in UNLV policy titled *Risk Assessment and Management*.

POLICY STANDARD: IS02-2 Security Level Classification. All UNLV information collections shall be classified as to its security level. Security Level classification shall be accomplished using the Handbook for Information Asset Classification, Part 1 (Step 3).

If the collections are automated, information system IT managers are responsible for applying the security level classification to the hosting IT systems under their jurisdiction and applying this

information to any System Security Plan (SSP) and Risk Assessment initiatives that are required by policy.

POLICY STANDARD: IS02-3 System Classification. All UNLV information collections, manual or automated, shall be classified according to the impact on it's security objective.. System classification shall be accomplished using the Handbook for Information Asset Classification, Part 2.

If the collections are automated, information system IT managers are responsible for applying the security categorization to the hosting IT systems under their jurisdiction and applying this information to any System Security Plan (SSP) and Risk Assessment initiatives that are required by policy.

POLICY STANDARD: IS02-4 Disaster Recovery Plan. All UNLV information systems with a System Classification as "moderate" or "high", or containing a information IT data-set or database with a Data Classification Criticality of "Required" or "Essential" shall have a Disaster Recovery Plan (see related UNLV IT Policy).

POLICY STANDARD: IS02-5 Compliance With Law And Policy. University departments, units, or IT groups should establish operational security guidelines, standards, or procedures that refine the provisions of this Policy for related data and systems, manual or automated, under their purview, in conformance with this Policy and other applicable policies and laws. Electronic information resources used in support of University business administration must comply with the provisions of Federal and state laws that prohibit theft or abuse of computers and other electronic resources.

ANNEX 1 –ROLES AND RESPONSIBILITIES

Executive Sponsor or persons acting in that capacity must:

- identify the information resources within areas under their control;
- define the purpose and function of the resources and ensure that requisite education and documentation are provided to the campus as needed;
- understand and ensure the compliance of regulatory statutes, regulations and policies that apply to the information resources under their responsibility;
- establish acceptable levels of risk for resources by assessing factors such as:
 - how sensitive the data is, such as research data or information protected by law or policy,
 - the level of criticality or overall importance to the continuing operation of the campus as a whole, individual departments, research projects, or other essential activities;
 - how negatively the operations of one or more units would be affected by unavailability or reduced availability of the resources,
- establish the security level for resources;
- ensure compliance with relevant provisions of other UNLV policies for systems in support of University business administration;
- ensure that requisite security policies and standards are identified and implemented for the resources;
- Senior management and the Officers of the University are required to employ internal controls designed to safeguard UNLV assets including academic and business information.

(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)

Data Steward or persons acting in that capacity have the responsibility to:

- Identify the classification level of all University information within their organizational unit,
- Define and implement appropriate safeguards to ensure the confidentiality, integrity, and availability of the information resource,
- Monitor safeguards to ensure their compliance and report situations of non-compliance,
- Authorize access to those who have a business need for the information,
- Remove access from those who no longer have a required business need for the information.

(These are University managers or directors of an organizational unit, department, etc. where the information is created, or that is the primary user of the information)

Data Administrator or persons acting in that capacity is designated by the Data Steward.

(These are the authorized University support persons or organization responsible for maintaining the safeguards established by the Data Steward)

Data Users or persons acting in that capacity must use the safeguards established by the Data Steward.

(These are the University employees or persons authorized by the Data Steward to access information)

University Information Security Officer or persons acting in that capacity has the responsibility to:

- The development and maintenance of University security policies, ensuring that security polices are implemented consistently across the University.
- Providing guidance to Executive Sponsors as they assess confidentiality, integrity and availability objectives for data under their control.
- Providing guidance to Data Stewards and Data Administrators as they assess confidentiality, integrity and availability objectives for data under their control.
- Reviewing the effectiveness of security-related implementation efforts with University IT Providers/IT Groups.
- Keeping abreast of privacy protection compliance and security related issues internally within the University community and externally throughout the information technology and security marketplace.
- Keeping abreast of privacy protection compliance issues, information assurance, information security threats, and general cyber-security throughout the related Sate and Federal Homeland Security and law enforcement communities.

(This the primary individual responsible for University information security oversight, privacy protection compliance auditing, or that is the primary auditor of information security safeguards and practices)

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

- become knowledgeable regarding relevant risk management requirements and guidelines;
- analyze potential threats and the feasibility of various security measures in order to provide security recommendations to Executive Sponsors;
- implement security measures that mitigate threats, consistent with the level of acceptable risk established by Executive Sponsors;
- establish procedures to implement relevant provisions of other UNLV policies for systems supporting University business administration;
- communicate the purpose and appropriate use for the resources 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)

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

(The roles of UNLV Executive Sponsors, Data Stewards, and Data Administrators are fully defined in the University data policy in the UNLV Office of Institutional Analysis and

Planning.)

Insufficient risk management 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.)