



OFFICE OF INFORMATION TECHNOLOGY

**CAPSTONE
POLICY - IS01**

**INFORMATION SECURITY FOR
INFORMATION RESOURCES AND ASSETS**

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 conjunction with the other Capstone policies, defines 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

The immutable purpose of the University of Nevada, Las Vegas (UNLV) information security policy is to protect all UNLV information assets (technology platforms, applications, and informational collections) against all internal, external, deliberate or accidental threats or misuses by using technology and

practices to mitigate risks associated with using information technology. It includes all UNLV networks and systems perimeter security, ongoing IT operations surveillance, and protection of critical, privacy, or sensitive data at rest or in transit. This UNLV Capstone Information Security Policy directly supports and effects the UNLV implementation of the NSHE Board of Regents Bylaws (Title 4, Chapter 1, Section 27 titled Data Security Policy).

SCOPE AND APPLICABILITY: Information is a significant asset of UNLV. The information technologies covered by the policy include systems, networks, and facilities administered by individual schools, departments, University laboratories, and other University-based entities. The University's information, excluding third-party intellectual property, includes information that is electronically generated, printed, filmed, typed, stored, or verbally communicated. The objective is to ensure a secure and protective information technology infrastructure that promotes the mission and business objectives of the University in research, teaching, learning, patient care, and administration. *The intent and the letter of the policy and all approved support policies shall be followed.*

The principles of confidentiality, integrity, and availability (CIA) shall be applied to all University information, the physical assets/systems that contain it, and the infrastructure that supports it. These assets, therefore, must be protected according to each asset's 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 distributed. Information identified as the property of third-parties that has been entrusted to the University shall also be safeguarded in accordance with this policy and in accordance with related agreements.

The security goal shall be 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. To achieve the goal the policy will be technologically based on an integrated or seamless defense-in-depth security model as the standard for all UNLV IT networks and systems constituents. The model provides for a layered and zoning capability for escalation of security controls to match an escalation of computer attacks or new compliance requirements.

The University, therefore, seeks to enforce its policies regarding privacy, harassment, and the safety of individuals; to protect the university against seriously damaging or legal consequences; to prevent the posting of proprietary software or the posting of electronic copies of literary and other works in disregard of copyright restrictions or contractual obligations; to safeguard the integrity of computers, networks, and data, either at UNLV or elsewhere; 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.

In concert with the intent of the Policy:

- All information resident on UNLV assets, including the assets, shall be classified according the UNLV Asset Classification Policy.
- All campus IT managers are directly responsible for implementing the global and derived policies and ensuring staff compliance in their respective departments or organizations.
- The use of IT systems will be consistent with sound security principles.
- IT systems will be used for their intended purposes and meet any compliance requirements.
- The five key principles of information security will be adhered to. These principles are:

(1) Principle of least privilege; (2) Principle of complete mediation; (3) Principle of openness of design; (4) Principle of the separation of duties; and (5) Principle of economy of mechanism.[see "Definitions" for the meaning of these terms.]

- The core IT network and systems will be available to support emergency services in the event of community disaster response needs.

Toward these ends, all faculty, staff, contractors, volunteers, and students have a responsibility for the security and protection of information and information technology devices owned by or administered by UNLV.

The UNLV Provost, with the advice of a senior level steering arch-committee chaired by the UNLV Chief Information Security Officer (CISO), is responsible for the oversight of the policy. It is the responsibility of the Office of Information Technology (OIT) to administer and maintain this Policy and approved related subordinate information security policies. ***Information security within UNLV will be implemented and managed through the creation and support of a Information Security Management System (ISMS) as defined by the International Standards Organization's ISO 17799 standard.*** The senior level steering arch-committee and the CISO shall oversee the ISMS and all sub-committees established to assist in the implementation of the ISMS.

BACKGROUND: The UNLV Provost's Office of Information Technology (OIT) administers and maintains the UNLV campus-wide network environment to meet the research, academic, privacy, and administrative needs of the UNLV campus community by providing applicational and related computing services, Internet access, integrated email and core security services. The high-level Global Information Security Policy and it's 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,
- UNLV contractual agreements with other legal entities,
- NSHE Board of Regents Bylaws (Title 4, Chapter 1, Section 27 of 2006) and
- other Federal and State of Nevada acts, laws, and regulations.

In order to manage information security comprehensively, this policy will serve four major purposes:

1. It creates an overarching or global information security policy for the University.
2. It establishes the principle that every information technology (IT) device connected to the UNLV network must have at least one individual managing the security of that device.
3. It requires organizations to designate a coordinating unit security person(s).
4. It requires an information security infrastructure with specific obligations and responsibilities regarding the security of information, information technology devices, and applications.

POLICY STANDARDS AND CONTROLS: See the ANNEX for POLICY 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. Additional subordinate tiers of information security policies, standards, and directives, will focus on common security standards for low-impact systems and

specific technological and application security standards for both moderate-impact and high-impact systems. The structure will 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;
- Appropriate information security training will be available for all members;
- All actual or suspected information security breaches will be reported to the OIT Information Security Office and will be thoroughly investigated.

COMPLIANCE: Policy compliance and enforcement requirements are:

1. UNLV administration has responsibility for the management of 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.

INFORMATION SECURITY BASELINE REFERENCE STANDARDS: The UNLV Information Security Policy and its structure shall be based on *International Standards Organization's 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, and the Generally Accepted Information Security Principles (GAISP). 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 its replacement.

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 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)

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 its 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 & 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

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

Least Privilege: The principle of least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to a domain with those privileges and nothing more. By denying to subjects transactions that are not necessary for the performance of their duties, those denied privileges cannot be used to circumvent the organizational security policy. The function of the user (as opposed to the users identity) should control the assignment of rights. If a specific action requires that a subject's access rights be augmented, those extra rights should be relinquished immediately upon completion of the action. This is the analogue of the "need to know" rule: if the subject does not need access to an object to perform its task, it should not have the right to access that object.

Complete Mediation: The principle of complete mediation states that every access to every object must be checked for authority. This principle, when systematically applied, is the primary underpinning of the protection system. It forces a system-wide view of access control, which in addition to normal operation includes initialization, recovery, shutdown, and maintenance. It implies that a foolproof method of identifying the source of every request must be devised. It also requires that everything be balanced: all accesses must be assigned as either allowed or disallowed – overlaps or gaps are not created.

Openness of Design: The principle of openness of design states that the security of a mechanism should not be dependent on secrecy or proprietary of design or implementation. Open design in the context of security means that developers, architects, and security personnel should base security designs on open standards that are used and reviewed by the industry. One of the benefits has been interoperable security standards. Security should rely on these open standards because systems, services, and data security assertions may be generated, recognized, and consumed by different, disparate technologies and protocols. Open standards are one way towards a common framework for interoperability, and most likely the most practical way.

Separation of Duties: The principle of separation of duty, also known as separation of privilege, can be either static or dynamic. Compliance with static separation requirements can be determined simply by the assignment of individuals to roles and allocation of transactions to roles. Allocating access rights according to role is also helpful in defining separation of duty in a way that can be enforced by the system. A static policy could be implemented by ensuring that no one who can perform the initiator role could also perform the authorizer role. A dynamic policy allows the same individual to take on both initiator and authorizer roles, with the exception that no one could authorize payments that he or she had initiated. The static policy could be implemented by checking only roles of users; for the dynamic case, the system must use both role and user ID in checking access to transactions.

Economy of Mechanism: The principle of economy of mechanism requires that the security design and implementation be as simple and small as possible. This well-known principle applies to protection mechanisms for this reason: fewer possibilities exist for errors. The checking and testing process is less complex, because fewer components and cases need to be tested.

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.

POLICY STANDARD: IS01-1 Logical Security. Computers must have the most recently available and appropriate software security patches, commensurate with the identified level of acceptable risk. Adequate authentication and authorization functions must be provided, commensurate with appropriate use and the acceptable level of risk. Attention must be given not only to large systems but also to smaller computers which, if compromised, could constitute a threat to campus or off-campus resources, including computers maintained for a small group or for an individual's own use.

POLICY STANDARD: IS01-2 Physical Security. Appropriate controls must be employed to protect physical access to resources, commensurate with the identified level of acceptable risk. These may range in scope and complexity from extensive security installations to protect a room or facility where server machines are located, to simple measures taken to protect a user's display screen.

POLICY STANDARD: IS01-3 Privacy And Confidentiality. University organizations shall implement appropriate technical and organizational measures to protect the privacy and confidentiality of sensitive data, including the processes applied to the data, against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access 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 must be in place at the destination computer to protect this "downstream data".

POLICY STANDARD: IS01-4 Compliance With Law And Policy. Campus departments, units, or groups should establish 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..

POLICY STANDARD: IS01-5 Security Controls and Practices. Information security controls and practices must be guided by risk assessment and the potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The FIPS 199 provides standard impact definitions that will be used within the UNLV information security policies. The application of the FIPS 199 impact definitions must be applied within the context of each organization and the overall University interest. A copy of the "FIPS 199 impact definitions" is contained in the Annexes to the policy document.

POLICY STANDARD: IS01-6 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, employee identification 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."

POLICY STANDARD: IS01-7 Security Breach Processing. University organizations shall identify and respond to suspected or known information security incidents; mitigate, to the extent practicable, harmful effects of the security incident that are known; collect and preserve necessary and appropriate legal evidence using standard "best practices"; and document security incidents and their outcomes.

POLICY STANDARD: IS01-8 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.

INFORMATION SECURITY TOPIC-SPECIFIC (TECHNICAL) POLICIES AND STANDARDS.

There shall be a Tier 2 level of policies and best-security-practices defined as topic-specific, such as firewalls, policies that set forth specific standards with any appropriate guidelines and procedures. These support security policies focus on specific technology areas of relevance and concern to UNLV. Each topic-specific policy sets a baseline composed of "common security standards" for low-impact systems. Additional standards directives may be defined for systems that are assigned "moderate-impact or high-impact" status. These policies are subject to more frequent revisions as changes in technology and other factors dictate. Examples of these focus areas are firewalls, anti-virus, intrusion protection, etc. These policies are generally found in the 100, 400, 500, 600, and 800 series of UNLV IT Policies.

INFORMATION SECURITY APPLICATION-SPECIFIC (APPLICATIONAL) POLICIES AND STANDARDS.

There shall be a Tier 3 level of policies and best-security-practices defined as application-specific, such as payroll systems, policies that set forth specific standards with any appropriate guidelines and procedures. These support security policies focus on a specific system or application of concern to UNLV. Each application-specific policy, frequently subordinate to a Tier 2 policy, sets a baseline composed of "common security standards" for low-impact applications. Additional standards directives may be defined for those applications that are assigned "moderate-impact or high-impact" status. Examples of these focus systems are payroll, financial records, purchasing, student

records, etc. These policies are generally either within or supportive of the 200 and 300 series of UNLV IT Policies.

ANNEX 2 –ROLES AND RESPONSIBILITIES

Administrative Officials or individuals 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)

Providers or individuals 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 individuals who design, manage, and operate campus electronic information resources, e.g. project managers, system managers, system designers, application programmers, or system administrators)

Users (individuals who access and use campus electronic information resources) 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.

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.)

ANNEX 3 –FIPS 199 IMPACT DEFINITIONS

The FIPS 199 impact definitions referenced by the Policy Standard for *Security Controls and Practices* are:

The *potential impact* is **LOW** if the loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law. AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The *potential impact* is **MODERATE** if the loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The *potential impact* is **HIGH** if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.