



OFFICE OF INFORMATION TECHNOLOGY
SPECIAL PUBLICATIONS, MANUALS, AND GUIDES

- UNLV Internal use ONLY -

HANDBOOK FOR INFORMATION ASSET CLASSIFICATION

RECOMMENDATIONS OF THE UNLV
OFFICE OF INFORMATION TECHNOLOGY
INFORMATION SECURITY OFFICER
FOR PERFORMING
UNLV INFORMATION CLASSIFICATION.

- UNLV Internal use ONLY -

TABLE OF CONTENTS

ASSET CLASSIFICATION	2
<i>INTRODUCTION.....</i>	<i>2</i>
PART 1: DATA/INFORMATION CLASSIFICATION.....	4
STEP 1: DESIGNATION OF SENSITIVITY LEVELS.....	4
STEP 2: DESIGNATION OF CRITICALITY LEVELS.....	5
<i>Background - Federal Requirements for Information Security and Protection.....</i>	<i>6</i>
STEP 3: INFORMATION SECURITY LEVEL STANDARD.....	6
<i>Table 1 - Information Categories Mapped To Information Security Levels</i>	<i>7</i>
<i>Table 2 - Information Security Levels Reference.....</i>	<i>8</i>
PART 2: IT SYSTEM CLASSIFICATIONS BY SECURITY OBJECTIVE IMPACT	9
ASSIGN POTENTIAL IMPACT BY SECURITY OBJECTIVE.....	9
<i>Step 1: Security Objective Impact Classification.....</i>	<i>9</i>
<i>Step 2: Determine Security Categorization (SC) for Information Types</i>	<i>10</i>
<i>Step 3: Determine Security Categorization (SC) for IT Information Systems.....</i>	<i>11</i>
ASSET CLASSIFICATION WORKSHEET	13

Asset Classification

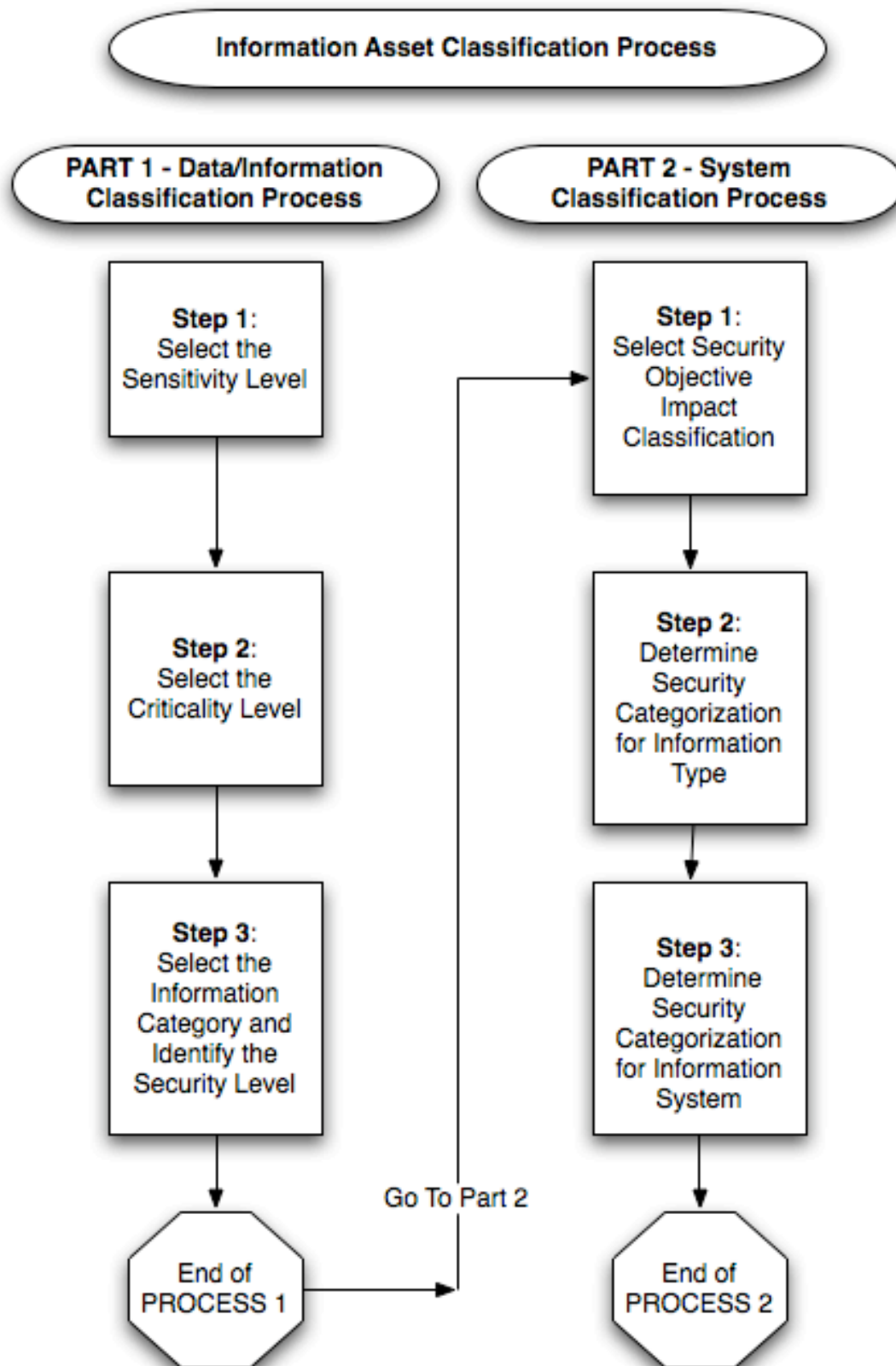
Introduction

An information asset or "system" may be a physical office, a file cabinet, or a IT system. The overarching handling process for UNLV's information asset inventory and classification is a set of guidelines that shall be applied to each data collection and IT system/device. Information security efforts are based on risk management of 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 processing systems.

The Data or Information Classification designations are grouped as Sensitivity and as Criticality, and each designation has multiple levels. The Security Level designations of the information collections and of the IT systems are used to define the requirements of UNLV's integrated security efforts.

The outcome or objective of the end Asset Classification is an assignment that will be used to establish the appropriate level, and cost, of information security necessary to safeguard the University's information assets and to comply with regulatory mandates.

NOTE: To determine appropriate and reasonable safeguards (what needs to be done and what needs to be provided) a baseline risk assessment must also be conducted (see UNLV Policy on Risk Assessment and Management).



PART 1: DATA/INFORMATION CLASSIFICATION

UNLV Information security efforts are based on the need to identify, classify, and protect sensitive information. The data classification level helps determine the minimum security safeguards required to protect this data and to ensure the operational continuity of critical information processing capabilities. An information asset, for the purposes of this document, may be a physical office, or a file cabinet with paper files, or an IT data collection system, or a digital database.

There are three levels of sensitivity and three levels of operational criticality. An information asset may be compartmentalized, such that a given data-set or process is more sensitive than other data-sets or processes. The information asset classification analyst should assign the highest level designation of any single data-set or process within the information system for the overall data classification level designation. A worksheet is located at the end of this handbook and may be used to record the assessment.

This practice supports the Information Security Office requirement to assign a security level impact to each Confidentiality, Integrity, and Availability (CIA) security objective – further information is in the System Classification guideline in Part 2.

STEP 1: Designation of Sensitivity Levels

Sensitivity classification of data is the need to help protect data from unauthorized disclosure, fraud, waste, or abuse. All UNLV data has some degree of sensitivity, even data that is intended for unrestricted access by many and varied individuals and groups. Additionally, UNLV is so dependent upon computers and networks that these capabilities are considered critical to some degree, otherwise resources would not be applied to managing them. Below is a list of examples of sensitive information. These may be physical or digital:

- Grant applications and Pre-contract award information
- Ongoing confidential research
- Performance review information for UNLV personnel
- Patient records
- Personnel records
- Arrest/crime records at UNLV
- Information regarding funding and budgets

Sensitivity levels are determined by the information type, **Unrestricted-Public, University-Confidential** or **Restricted**, that is in an information collection or system. Level 1 applies to information with the least amount of sensitivity and Level 3 applies to information with the greatest amount of sensitivity.

Select one of the three Sensitivity Levels (SL) below which best describes or most closely matches the information collection or asset.

Level SL1 or Unrestricted-Public Sensitivity information requires a minimal amount of protection. This level includes information that is considered to be in the public domain or does not fit into the other levels, such as employee campus contact files. At this level, any disclosures could be reasonably expected not to have an adverse effect. But remember that all information is important, otherwise it would not be collected. Unintentional alteration or destruction is the primary concern for this sensitivity information.

Level SL2 or University-Confidential Sensitivity information covers the internal information at UNLV and requires strong security safeguards at the user level and therefore must be protected against acts that are considered to be malicious and destructive. Level 2 Sensitivity data could include:

1. Computerized correspondence and document files that are regarded as highly sensitive and/or critical to an organization whose release or distribution outside the University department and/or within UNLV needs to be controlled.
2. Proprietary information that has inherent informational value, such as formulas and early research findings.
3. Financial data that is used to authorize or make payments to individuals or organizations.
4. Grant application data.
5. Academic or department information that pertains to teaching, workload, staffing, general correspondence and memoranda, and other document files.
6. Data that must be protected from unauthorized alteration and/or disclosure.

Level SL3 or Restricted Sensitivity information covers the most sensitive information at UNLV and requires the greatest security safeguards at the user level. Level 3 Sensitivity data could include:

1. Proprietary information that has inherent informational value, such as drug formulas, trade secrets, and early research findings requiring extra protection.
2. Clinical trial data.
3. Automated systems or records subject to the Federal or State Acts for which unauthorized disclosure would constitute a clearly unwarranted invasion of personal privacy or contribute to a possible identity theft issue.
4. Technical information concerning the internal operation, protection, and security methods of the University's Level 2 and Level 3 IT networks and systems.
5. Data that must be protected from unauthorized disclosure by mandate of law or regulation.

STEP 2: Designation of Criticality Levels

Operational criticality of IT capabilities is the assessment of what if the processing capabilities were interrupted for a period of time or subject to fraud or abuse. In addition to the sensitivity levels above, IT processing capabilities are assigned criticality levels. These correspond to the relative importance of the automated capability in accomplishing UNLV's mission. Level 1 applies to capabilities with the least amount of criticality and Level 3 applies to automated capabilities with the greatest amount of criticality. These criticality levels are used to help determine the appropriate level of protection for automated information capabilities.

Select one of the three Criticality Levels (CL) below based on which most closely matches the information collection or asset.

Level CL1 or Deferrable Criticality refers to an automated information system, computer or network that users only need to take minimal precautions to protect. In the event of an alteration or failure, the loss of this data processing capability would affect the organization minimally, and/or this information could be replaced with minimum staff time and expense. This level processes no data categorized higher than Level 1 Public sensitive.

Level CL2 or Required Criticality identifies an automated information system, computer or network that is considered important, but not imperative, to UNLV's internal management or the department. If a

moderately critical computer system is unable to function for an extended period of time, it would not have a devastating impact on the organization it supports.

Level CL3 or Essential Criticality refers to an automated information system, computer or network essential to the organization. At this level, if the system, computer or network is unable to function for even a short period of time, it could have a severe impact on the organization. An example of a highly critical UNLV asset is one that affects a significant mission or a large number of UNLV employees or departments when it is unavailable.

Background - Federal Requirements for Information Security and Protection

Health Insurance Portability and Accountability Act (HIPAA) of 1996

HIPAA regulates national standards for protecting the privacy of Americans' personal health records. The regulation states that it is the responsibility of organizations that are entrusted with health information to protect it against deliberate or inadvertent misuse or disclosure.

Family Education Rights and Privacy Act (FERPA) of 1974

FERPA protects student records. This act protects student information from all organizations and personnel, including parents, unless student grants authorization.

Privacy Act of 1974

This act protects information about individuals from public scrutiny. For records to fall under the purview of the Privacy Act, they must be:

- *Part of an established Privacy Act system of records (published in the Federal Register).*
- *Retrieved by the name of the individual or by some unique identifying number or symbol that is linked to the name.*
- *Records that are under the control of the UNLV.*

Financial Modernization Act of 1999 also known as the **Gramm-Leach-Bliley Act (GLB Act)**,

*This act includes privacy provisions to protect consumer information held by financial institutions. In 2003, the Federal Trade Commission (FTC) confirmed that higher education institutions are considered financial institutions under this federal law. The **Safeguards Rule [16 CFR Part 314] of the GLB Act** requires financial institutions to have a security plan to protect confidentiality and integrity of personal information. Privacy notices explaining an institution's information-sharing practices must also be provided.*

STEP 3: Information Security Level Standard

System Owners/Managers must determine the appropriate system security level based on (1) the confidentiality, integrity and availability objectives of the information, and (2) based on the data sensitivity and its criticality to the department's university/business mission. This is the basis for assessing the risks to UNLV operations and assets and in selecting appropriate security controls and techniques.

The standard for information Security Levels establishes common criteria for assigning security levels to an information category. The first table below defines the Security Levels. The second table below lists Security Levels for various information categories. (Note: that business-critical information is its own category). The system owner locates his/her information category to find the appropriate system Security Level. In the cases where information of varying security levels are combined, the highest security level takes precedence. Where system availability or data integrity are of high importance, see the table footnote.

System Owners/Managers and System Support/Developers must ensure that their information collections or databases and the processing capabilities of their systems are accessed only by authorized users who fully use the required security level safeguards. The Security Level designation will be used to determine the minimum-security safeguards required to protect sensitive data and to ensure the operational continuity of critical data processing capabilities.

Select the Information Category based on which most closely matches the information collection or asset in column 1 and identify the designated Security Level (ScL) in column 3.

Table 1 - Information Categories Mapped To Information Security Levels

Information Category	Category Explanation and Examples	System Security Level (ScL)*
Investigation and security information	Information related to investigations for law enforcement or security purposes that cannot be classified, but is subject to confidentiality and extra security controls. Includes security plans, contingency plans, emergency operations plans, incident reports, reports of investigations, risk or vulnerability assessments certification reports; does not include general plans, policies, or requirements.	High
Business-critical information	Information designated as critical to a department's mission, includes vital information for emergency operations.	High
Life-critical information	Information critical to life-support systems (i.e., information where inaccuracy, loss, or alteration could result in loss of life).	High
Information about persons	Information related to personnel, medical, and similar data. Includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), EEO, personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history), FERPA, etc.	High
Financial, budgetary, commercial, proprietary and trade secret information	Information related to financial information and applications, commercial information received in confidence, or trade secrets (i.e., proprietary, contract bidding information, sensitive information about patents, and information protected by agreement. Also included is information about payroll, automated decision making, procurement, inventory, other financially-related systems, and site operating and security expenditures.	Moderate
Internal administration	Information related to the internal administration of an agency. Includes personnel rules, bargaining positions, and advance information concerning procurement actions.	Moderate
Operational information	Information that requires protection during operations; usually time-critical information.	Moderate
System configuration management information	Any information pertaining to the internal operations of a network or computer system, including but not limited to network and device addresses; system and protocol addressing schemes implemented at an agency; network management information protocols, community strings, network information packets, etc.; device and system passwords; device and system configuration information.	Moderate

Public information	Any information that is declared for public consumption by official authorities. This includes information contained in press releases approved by the Office of Public Affairs or other official sources. It also includes Information placed on public access world-wide-web (WWW) servers.	Low
Other sensitive information	Any information for which there is a management concern about its adequate protection, but which does not logically fall into any of the above categories. Use of this category should be rare.	Low

* The level is based on data sensitivity requirements for the information system. The low system security level may be increased to moderate (not to high) if the information system has significant integrity and/or availability requirements. The moderate level cannot be increased to high. See Table 2 for explanations of the security levels.

Table 2 - Information Security Levels Reference

Security Level (ScL)	Description	Security Level Explanation
Low	Limited	Noticeable impact on an department's missions, functions, image, or reputation. A breach of this security level would result in a negative outcome; or would result in DAMAGE, requiring repairs, to an asset or resource.
Moderate	Serious	Significant impairment to a department's missions, functions, image, and reputation. The impact would place an agency at a significant disadvantage; or would result in MAJOR DAMAGE, requiring extensive repairs, to assets or resources.
High	Severe or Catastrophic	Complete loss of mission capability for an extended period; or would result in the MAJOR LOSS of assets or resources and could pose a threat to human life.

PART 2: IT SYSTEM CLASSIFICATIONS BY SECURITY OBJECTIVE IMPACT

While Part 2 focuses primarily on the IT components, it is still a good idea to perform the analysis on all information collections to understand the physical security that may be needed. The systems security efforts of the IT Information Security Program are based on the sensitivity of data contained in all systems, and the operational criticality of the data processing capabilities of those systems. The most critical information assets are the data recorded in these assets, such as financial, student, patient and treatment records. University organizations must implement appropriate and reasonable safeguards to protect the Confidentiality, Integrity, and Availability of UNLV information assets where needed.

Impact analysis and measurement is given the term "security categorization" or SC. This analysis is used to categorize LOW, MODERATE, and HIGH security risks to the security objectives of Confidentiality, Integrity, and Availability. The analysis conducted by the organization will identify the impact that the loss of Confidentiality, Integrity, and Availability would have on the ability of the UNLV organization to accomplish its mission or the harm that would be caused.

The analysis should identify the impact for both short-time and extended-time loss or outage. A single system could be designated Deferrable, Required, or Essential (see Criticality Levels in Part 1) depending on how long it is unavailable or the outage lasts. The summary below will help you identify risks to particular information or processes or systems.

The impact designation determines the minimum security safeguards required to ensure the operational continuity of critical information processing capabilities. The Data Classifications from Part 1 should be used as input to determine the System Classification. NOTE: An information system may be compartmentalized, such that a given information collection or process is more sensitive than other information-sets or processes. The information manager should assign the highest security level designation of any information-set or process within the information system as the overall security level designation – this is referred to as a "System High" rating.

Assign Potential Impact By Security Objective

Step 1: Security Objective Impact Classification

For each information type (**Unrestricted-Public**, **University-Confidential** or **Restricted**) classify the "System Security Level" or potential impact by assigning a HIGH, MODERATE, or LOW impact classification to each of the three security objectives.

CONFIDENTIALITY

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

1. **Class=LOW** if the unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.
2. **Class=MODERATE** if the unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
3. **Class=HIGH** if the unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

INTEGRITY

Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

1. **Class=LOW** if the unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.
2. **Class=MODERATE** if the unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
3. **Class=HIGH** if the unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

AVAILABILITY

Ensuring timely and reliable access to and use of information.

1. **Class=LOW** if the disruption of access to or use of an information collection could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.
2. **Class=MODERATE** if the disruption of access to or use of an information collection could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
3. **Class=HIGH** if the disruption of access to or use of an information collection could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Step 2: Determine Security Categorization (SC) for Information Types

The security category of an information type (**Unrestricted-Public, University-Confidential or Restricted**) can be associated with both user information and system information and can be applicable to information in either electronic or non-electronic form. It can also be used as input in assigning the appropriate security category of an IT system (see description of security categories for information systems below). Establishing an appropriate security category of an information type essentially requires using the *potential impact classification* for each security objective from Step 1 above. (*IT system information (e.g., network routing tables, password files, and cryptographic key management information) must be protected at a level commensurate with the most critical or sensitive user information being hosted, processed, stored, or transmitted by the information system to ensure proper Confidentiality, Integrity, and Availability.*)

The generalized format for expressing the security category, or SC, of an information type is:

SC information type = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE. The potential impact value of *not applicable* only applies to the security objective of confidentiality.

EXAMPLE 1: An organization managing *Unrestricted-Public information* on its web server determines that there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of

availability. The resulting security category, SC, of this information type is expressed as:

SC *unrestricted*-public information = {(confidentiality, NA), (integrity, MODERATE), (availability, MODERATE)} or the SC=MODERATE for the information.

Step 3: Determine Security Categorization (SC) for IT Information Systems

Determining the security category of an information system requires slightly more analysis and must consider the security categories of all information types resident on the information system. For an information system, the potential impact value assigned to the respective security objectives (Confidentiality, Integrity, Availability) shall be the highest value from among those security categories that have been determined for each type of information resident on the information system. It is recognized that information systems are composed of both programs and information. Programs in execution within an information system (i.e., system processes) facilitate the processing, storage, and transmission of information and are necessary for the organization to conduct its essential mission-related functions and operations. These system processing functions also require protection and could be subject to security categorization as well. However, in the interest of simplification, it is assumed that the security categorization of all information types associated with the information system provide an appropriate *worst case* potential impact for the overall information system—thereby obviating the need to consider the system processes in the security categorization of the information system.

The generalized format for expressing the security category, SC, of an information system is:

SC information system = {(confidentiality, impact), (integrity, impact), (availability, impact)},

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

Note that the value of *not applicable* cannot be assigned to any security objective in the context of establishing a security category for an IT information system. This is in recognition that there is a low minimum potential impact on the loss of Confidentiality, Integrity, and Availability for an IT information system due to the fundamental requirement to protect the operating system-level processing functions and information critical to the operation of the IT system itself.

EXAMPLE 2: An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. The management within the contracting organization determines that: (i) for the sensitive contract information, the potential impact from a loss of confidentiality is moderate, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is low; and (ii) for the routine administrative information (non-privacy-related information), the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low. The resulting security categories, SC, of these information types are expressed as:

SC contract information = {(confidentiality, MODERATE), (integrity, MODERATE), (availability, LOW)},

and

SC administrative information = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}.

The resulting security category of the information system is expressed as:

SC acquisition system = {(confidentiality, MODERATE), (integrity, MODERATE), (availability, LOW)}, or the SC=MODERATE for the acquisition system.

representing the system-high mark or maximum potential impact values for each security objective from the

information types resident on the acquisition system.

NOTE: To determine appropriate and reasonable safeguards (what needs to be done and what needs to be provided) a baseline risk assessment must also be conducted (see UNLV Policy on Risk Assessment and Management).

ASSET CLASSIFICATION WORKSHEET

INFORMATION COLLECTION NAME:

LOCATION:

DEPARTMENT:

EXECUTIVE SPONSOR:

DATA STEWARD:

DATA ADMINISTRATOR:

SENSITIVITY LEVEL (SL):

CRITICALITY LEVEL (CL):

SECURITY LEVEL (ScL):

SECURITY CATEGORIZATION (SC):

FOR AUTOMATED SYSTEMS ONLY:

DEPARTMENT PROVIDING IT SUPPORT:

SERVER NAME & LOCATION:

SYSTEM ADMINISTRATOR & LOCATION:

DATABASE ADMINISTRATOR & LOCATION:

SYSTEM SECURITY ADMINISTRATOR & LOCATION:

IT SUPPORT EQUIPMENT LIST (ROUTER, FIREWALL, ETC.):

NOTE: To determine appropriate and reasonable safeguards (what needs to be done and what needs to be provided) a baseline risk assessment must also be conducted (see UNLV Policy on *Risk Assessment and Management*).