UNLV | Office of INFORMATION TECHNOLOGY

UNLV Data Classification Levels

April 2017

Information Security Office
UNLV OIT

Overview

Classifying data allows UNLV to efficiently use its resources to secure its data. Applying the same security controls to all data is expensive and utilizes security resources on data that do not require extensive security controls.

For example, if an openly published course schedule is secured to the same level as a student health record, the openly published course schedule is more difficult to use and utilizes scarce security resources which are needed to make the student health record more secure.

Correctly classifying data is the first step in securing data in an efficient and cost effective manner.

Applicable Federal and Nevada Statutes

There are several laws that influence how UNLV should classify data. Some of the primary laws are:

- Nevada Public Records Act (NRS Chapter 239)
- Nevada Security of Personal Information Law (NRS Chapter 603A)
- Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. §1232g,)
- Health Insurance Portability and Accountability Act (HIPAA , Public Law 104-191)
- Gramm-Leach-Bliley Act (GLBA, Public Law 106-102)
- Export Administration Act of 1979 (EAR, Public Law 96-72)

Nevada Public Records Act (NRS Chapter 239)

The Nevada Public Records Act was implemented by the Nevada State Legislature to ensure public books and not otherwise declared by law to be confidential are available to the public for inspection or copying. The law sets forth the right to request inspection or copying, a government agency's responsibilities in responding to a request, and the remedies available to a requesting party in the event a request is denied.

Nevada Security of Personal Information Law (NRS Chapter 603A)

The Nevada Security of Personal Information Law defines what constitutes "personal information" and defines the security measures imposed upon those who deal with "personal information."

Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. §1232g)

The Family Educational Rights and Privacy Act ("FERPA") gives students and their parents the right to inspect and review all education records related to the student. In general, this law it defines "education record," and states that education records, and particular information contained within those records, in most circumstances must be kept private unless the parent or student consents to release of the records. A parent's right under this law is transferred solely to the student when the student reaches the age of eighteen (18) years old.

Health Insurance Portability and Accountability Act (Public Law 104-191)

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH") establish data privacy and security standards to protect an individual's medical records and personal health information.

Gramm-Leach-Bliley Act (Public Law 106-102)

The Gramm-Leach-Bliley Act, or Financial Modernization Act of 1999, requires financial institutions to openly publish their information-sharing practices to their customers. The act requires financial institutions, which includes educational institutions, to take appropriate safeguards to protect and keep private student financial information and data.

Export Administration Act of 1979 (Public Law 96-72)

The Export Administration Act of 1979 allows the President of the United States to control U.S. exports for the purposes of national security, foreign policy, and short supply. The act's supporting Export Control Regulations ("ECR"), managed by the U.S. Bureau of Industry and Security, control the export of sensitive technologies and resources. Typically, this act involves the control of resources or technologies that have dual civilian and military uses.

UNLV Data Governance Policy

The UNLV Data Governance and Management Policy details data handling at UNLV.

Data Steward Responsibilities

The data steward holds an essential role in any data classification system. The data steward is responsible for determining the classification of data. Typically, the data steward is the person or organization that created the data.

Ultimately, the owner of all data at UNLV is UNLV. However, it is the responsibility of each UNLV faculty or staff member to manage any UNLV data they create and/or curate in the best interests of UNLV, and in accordance with the UNLV Data Classification System.

The Data Classification System for UNLV

UNLV's data classification system consists of three levels: Restricted Data, Internal Data, and Public Data.

Restricted Data

[redacted]

Restricted Data is institutional data of a highly sensitive nature and whose inappropriate handling or disclosure could result in detrimental consequences for the university and individuals associated with the institution. This data warrants the administration of stringent security measures, and access should be limited to only university employees with a demonstrated business need. Because restricted data is typically subject to federal or state regulations, a security breach would require the institution to notify the affected individual(s) as well as law enforcement authorities. Examples of Restricted Data include data protected by State or Federal privacy laws and regulations or NSHE code provisions data subject to export controls, proprietary information, trade secrets, or data protected by confidentiality agreements. The highest level of security controls should be applied to **Restricted Data**.

Internal Data - The Default Classification

Internal Data is institutional data intended to be protected from external dissemination and public consumption on account of business, regulatory, and ethical concerns. Selective access to particular elements or subsections of this data is provided to individuals from the university community and affiliated organizations that possess a business need for the data in order to carry out their required job duties or satisfy their role at the institution. **Internal Data** may be released to the individuals outside the university community only with approval from the data steward, designated executive sponsor, or when required by law. Examples of internal data include employee identification numbers, faculty and staff personnel records, student admission and enrollment records, and purchase requisition records.

Public Data

Public Data is institutional data approved for release to members of the university community and external parties (including the general public and the media) without access restrictions because the data's disclosure poses little or no risk to the university, affiliated individuals, or non-affiliated persons. Examples of public data include names of university employees, their workplace email addresses, their workplace telephone numbers, and other directory information as well as aggregated information available on the UNLV Official website without user authentication.

Data Access By Classification

Data classification drives the security controls required for a particular piece of data. Access becomes increasingly controlled as the classification level increases. In general, you must have a valid, documented business need to know information.

Restricted Data

Restricted Data access should be limited to only UNLV employees with a demonstrated business need or to individuals who have gone through appropriate channels to be authorized to have access to the data (e.g., external law enforcement in consultation with UNLV Police Services and/or General Counsel, contractors with appropriate confidentiality provisions in place, health insurance companies or other related companies which have appropriate business associate agreements in place).

Internal Data

Internal Data access is provided to individuals from the university community and affiliated organizations that possess a business need for the data in order to carry out their required job duties or satisfy their role at the institution. **Internal Data** may be released to individuals outside the university community only with approval from the data steward, designated executive sponsor, or when required by law.

Public Data

Public Data is institutional data explicitly approved for release to members of the university community and external parties (including the general public and the media) without access restrictions.

Periodic Review of Data Classification

All data stewards should review the data for which they are responsible once per year to determine if data classification levels need to be adjusted.

Specific Examples of Types of Data By Classification

Restricted Data

Examples of data classified as **Restricted Data** include, but are not limited to:

Patient Medical/Health Information (HIPAA)

- Social Security number
- Patient names, street address, city, county, zip code, telephone / fax numbers
- Dates (except year) related to an individual, account / medical record numbers, health plan beneficiary numbers
- Personal vehicle information
- Certificate / license numbers, device IDs and serial numbers, email, URLs, IP addresses
- Access device numbers (building access code, etc.)
- Biometric identifiers and full-face images
- Any other unique identifying number, characteristic, or code
- Payment Guarantor's information
- Medical treatment and billing records and related correspondence or notes

Student Education Records (FERPA)

Enrolled and prospective student data that include the following:

- Social Security number
- Grades including test scores, assignments, and course grades
- Student financial information, credit cards, bank accounts, wire transfers, payment history, financial aid, grants, and student bills
- Access device numbers (building access code, etc.)
- Biometric identifiers

- Date of birth

NSHE Defined FERPA Directory Information (when requested to be held private by a FERPA protected individual)

The Nevada System of Higher Education (NSHE) has defined the following student information as FERPA directory information:

- Name
- College
- Participation in officially recognized activities and sports
- Dates of attendance
- Address
- Date of graduation
- Telephone number
- Undergraduate or graduate student status
- Weight and height of members of athletic teams
- Most recent educational agency or institution attended
- Email address (university-supplied)
- Enrollment status (full-time or part time)
- Degrees, honors, and awards received
- Major field of study

FERPA Directory Information is considered **Public Data**, **unless the FERPA protected individual specifically requests that the data not be released**.

If a FERPA protected individual specifically requests that the Directory Information not be released, then the FERPA protected individual's Directory Information becomes **Restricted Data**.

Donor/Alumni Information (Nevada Security of Personal Information Law)

- Social Security number
- Driver's License Number
- Name
- Personal financial information
- Family information
- Medical information
- Credit card numbers, bank account numbers, description of donation (monetary or otherwise)
- Telephone / fax numbers, e-mail, URLs

Research Information (Export Control Laws, Granting Authority Agreements)

- Human subject information
- Sensitive digital research data
- Export Controlled Information – Information or technology controlled under the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR) as described below, is confidential.
    - Information which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of a controlled item or product. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation
    - Classified information relating to defense articles and defense services
    - Information covered by an invention secrecy order
    - Software directly related to a controlled item

Employee Information (Nevada Security of Personal Information Law and Nevada System of Higher Education Handbook)

- Personnel and payroll files
- Social Security number
- Date of Birth
- Driver's License Number
- Family information
- Insurance benefit information
- Access device numbers (building access code, etc.)
- Biometric identifiers

Business/Vendor Data (Gramm-Leach-Bliley Act, Non-Disclosure Agreement)

- Vendor social security number
- Personally identifiable financial information
- Credit card information
- Contract information between UNLV and a third party
- Access device numbers (building access code, etc.)
- Biometric identifiers
- Certificate / license numbers, device IDs and serial numbers, email, URLs, IP addresses

Other Institutional Data (Gramm-Leach-Bliley Act, Other Security Considerations)

- Physical plant detail
- Credit card number
- Driver's License number

- Critical infrastructure detail
- User account passwords
- User Identification Number (UIN)

Internal Data

By default, all University data which is not explicitly classified as **Restricted Data** or **Public Data** is considered to be **Internal Data**. **Internal Data** may be released to individuals outside the university community only with approval from the data stewards, designated executive sponsor, or when required by law.

Examples of data classified as **Internal Data** include, but are not limited to:

- Internal emails
- Internal operational documents
- Phone messages
- Phone records
- Internal departmental plans
- Internal meeting notes
- University or departmental policies under development
- Course descriptions for courses under development
- Syllabi for courses under development
- Schedules for courses under development
- Unpublished research data not explicitly classified as **Restricted Data**
- Computer usage records
- Maintenance records
- Purchase orders

Public Data

Public Data is data that the data steward has explicitly shared with the general public.

Examples of data classified as **Public Data** include, but are not limited to:

- Research posted by the data steward on publicly available websites
- Published research
- Published dissertations
- Published theses
- Course syllabi from offered courses

- Course descriptions from offered courses
- Class schedules
- Published and officially approved university policies

Summary

Classifying UNLV data is the first step in determining how best to secure that data.

When data is created, it is the responsibility of the data steward to classify that data and to ensure appropriate security controls are in place to protect that data. Data stewards must review the data for which they are responsible at least once per year to verify that the current data classification level is still appropriate.

Restricted Data is legally protected data under State or Federal laws and regulations and requires the highest level of security controls. The unauthorized release of **Restricted Data** can result in costly remediation and fines as well as damage to the university's reputation. The intentional release of **Restricted Data** can result in disciplinary action.

Internal Data is data that may be released to individuals outside the university community only with approval from the data steward, designated executive sponsor, or when required by law. Some data in this category may be a matter of public record in the State of Nevada.

Public Data is UNLV data that is explicitly made available to the general public and requires the lowest level of security control.

References

"Chapter 603A - Security of Personal Information" Nevada State Legislature, Nevada State Legislature, nd. Web nd.

"Family Educational Rights and Privacy Act (FERPA)" U.S. Department of Education, U.S. Department of Education, nd. Web nd.

"Gramm-Leach-Bliley Act" Federal Trade Commission, Federal Trade Commission, nd. Web nd.

"Guidelines for Data Classification" Carnegie Mellon University Information Security Office, Carnegie Mellon University Information Security Office, nd. Web nd.

"Individual's Right Under HIPAA to Access Their Health Information 45 CFR 164.524" U.S. Department of Health and Human Services, U.S. Department of Health and Human Services, nd. Web nd.

"Nevada Public Records Act: A Manual for State Agencies" Nevada State Library, Archives, and Public Records, Nevada State Library, Archives, and Public Records, nd. Web nd.

"Overview of U.S. Export Control System" U.S. Department of State, U.S. Department of State, nd. Web nd.

"UNLV Data Governance and Management Policy" UNLV, UNLV, 2016. Web 2016.

DISCLAIMER