

WNC Data Classification Levels

Updated: June 2, 2023

Overview

Applicable Federal and Nevada Statutes

[Nevada Public Records Act \(NRS Chapter 239\)](#)

[Nevada Security of Personal Information Law \(NRS Chapter 603A\)](#)

[Family Educational Rights and Privacy Act \(FERPA\)](#)

[Health Insurance Portability and Accountability Act \(Public Law 104-191\)](#)

[Gramm-Leach-Bliley Act \(Public Law 106-102\)](#)

[Export Administration Act of 1979 \(Public Law 96-72\)](#)

The Data Classification System for WNC

Specific Examples of Types of Data By Classification

Restricted Data

[Patient Medical/Health Information \(HIPAA\)](#)

[Student Education Records \(FERPA\)](#)

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

[Donor/Alumni Information \(Nevada Security of Personal Information Law\)](#)

[Employee Information \(Nevada Security of Personal Information Law and Nevada System of Higher Education Handbook\)](#)

[Business/Vendor Data \(Gramm-Leach-Bliley Act, Non-Disclosure Agreement\) Other](#)

[Institutional Data \(Gramm-Leach-Bliley Act, Other Security Considerations\)](#)

Internal Data

Public Data

Summary

References

Applicable Federal and Nevada Statutes

There are several laws that influence how WNC 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 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.

The Data Classification System for WNC

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

Restricted Data access should be limited to only WNC 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 WNC 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 access is provided to individuals from the college 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 college community only with approval from the data steward, designated executive sponsor, or when required by law.

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

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
- Date of Birth
- 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
- Student's prior tax transcripts/tax returns and W2
- Parents prior tax transcripts/tax returns and W2
- Biometric identifiers

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

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
- Biometric identifiers
- Employment applications
- Medical information
- Results of pre-employment screenings
- Results of continued employment screenings

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

- Vendor social security number
- Personally identifiable financial information
- Credit card information
- Contract information between WNC 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)

- Critical infrastructure detail
- User account passwords
- User Identification Number (UIN)
- Physical plant detail
- Credit card number
- Driver's License number

Internal Data

By default, all College 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 college 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
- College 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 is explicitly shared with the general public. Examples of data classified as Public Data include, but are not limited to:

- Course descriptions from offered courses
- Course syllabi from offered courses
- Class schedules
- Published and officially approved college policies
- FERPA Directory Information is considered Public Data, unless the FERPA protected individual specifically requests that the data not be released

Summary

Classifying WNC 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 college'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 college 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 WNC 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 College Information Security Office, Carnegie Mellon College 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.

DISCLAIMER

This WNC Data Classification Levels document is intended to be a guideline, and not a WNC policy document. It is subject to change, termination, updates, revisions, or amendments at any time with or without notice. Also, new guidance, policies and/or procedures regarding any subject matter contained herein may be adopted at any time with or without notice. This guidance document is not intended to and shall not be construed, interpreted, or relied on to classify or characterize any particular data as a public record or book pursuant to Nevada Revised Statutes Chapter 239 (the Nevada Public Records Act), or as otherwise available to the public. This guidance document shall not be construed as a waiver of any claim of confidentiality over any particular data mentioned therein. WNC makes no claims, promises, or guarantees about the accuracy, completeness or adequacy of the contents of this guidance document and expressly disclaims liability for errors or omissions contained within its content.