CHRISTOPHER NEWPORT
UNIVERSITY

Data Classification Standard

VERSION 1.5

June 2023

Department: Information Security

Proprietary Statement

This document was developed specifically for and by Christopher Newport University. The concepts and methodologies contained herein are proprietary to Christopher Newport University. Duplication, reproduction, or disclosure of information in this document without the express written consent of Christopher Newport University is prohibited.

All Trademarks, Registered Trademarks, Service Marks, and brand and product names used in this document are the property of their respective owners.

Review and Revision History

Date	**Version**	**Description of Change** **(Affected Sections)**	**Author**
November 2017	1.0	Initial Release - All	Nathan Bray
August 2018	1.1	Converted to a standard. Updated formatting and added definitions.	Andrew Crawford
April 2020	1.2	Annual Review	Wendy L. Corrice
June 2021	1.3	Annual Review	Wendy L. Corrice
June 2022	1.4	Annual Review and update to Data Classifications	Wendy Corrice
June 2023	1.5	Annual Review, added Scope and GLBA definition	Wendy Wilde

TABLE OF CONTENTS

Introduction

This standard meets the Commonwealth of Virginia's requirement that agencies develop policy and processes for access control to agency data.

The University intends that the data should be freely accessible within the framework established, while recognizing the University's responsibilities specified in the Commonwealth of Virginia's Information Security Management Standards (SEC 501 and SEC 525) and Federal Law (FERPA/HIPPA) to secure access to data. Therefore, the University has developed the following procedures to meet the Commonwealth's Information Security Standards.

According to the University's Unified Data Policy, sensitive University data must be protected against physical theft or loss, electronic invasion, or unintentional exposure through a variety of personal and technical means.

When classifying University data, the following criteria for individual data elements, applications or systems shall be used. If there is a question about which category data falls under, the highest possible category in classifying the data should be assumed. Although some or parts of the data listed may be subject to disclosure under the Virginia Freedom of Information Act, the following classifications still apply. If a Freedom of Information Act request for the release of data is received, University Counsel shall be consulted before responding to the request.

Scope

This standard includes:

- All data and systems supporting the business and operational needs of Christopher Newport University.
- Information and data in all forms, including but not limited to, information- processing activities, computerized data (whether stored on university-managed servers and storage, storage area network, local servers, personal workstations, or vendor-provided infrastructures such as a "cloud"), and manually maintained data files regardless of where those files are stored.
- All application, network, and operating system software used for computerized management of these data or systems.
- Computerized data-processing activities related to research and instruction where the Information Security Officer (ISO) determines that such activities should be covered by this standard.
- All data and systems owned by or within the control of the University.

Standard:

All institutional data is owned by Christopher Newport University. As such, all members of the University community have the obligation to appropriately secure and protect the asset in all formats and in all locations. Roles and responsibilities for protecting and classifying the institutional data asset are defined in supporting Information Technology Standards.

Data Classification Levels

The data classification levels are defined as follows and are listed in order from the most sensitive to the least sensitive.

a. ***Class 1 Restricted***

   i. Data classified as Class 1 (R*estricted)* may be subject to disclosure laws and warrant careful management and protection to ensure its integrity, appropriate access, and availability. This information must be guarded from disclosure. Unauthorized exposure of this information could contribute to identity theft, financial fraud, and violate state and/or federal laws. Unauthorized disclosure of this data could adversely affect the University, or the interests of individuals and organizations associated with the University. Systems containing *restricted* data must be approved by the Information Security Officer. Restricted data includes Social Security Number (SSN), Drivers License number, Federal ID, Health Insurance, Medical Record Number, Payment Card Holder Data, and Medical Information (PHI), when combined with identifying information.

   ii. Restricted data and systems should utilize measures such as encryption, two-factor authentication, or other added protections commensurate with the level of sensitivity and the compensating controls that are available.

   iii. If a file which would otherwise be considered *confidential* contains any element of *restricted* data, the entire file is considered to be *restricted* information.

b. ***Class 2 Confidential, Moderate Sensitivity***

   i. Data classified as Class 2 (*Confidential, moderate sensitivity)* includes data that is not explicitly defined as *restricted* data but that is regulated and requires access control and contract language for hosted solutions. This data is not intended to be made publicly available or shared without authorization. *Class 2* data is distributed on a need-to-know basis between members of the University staff, IT systems, and specific third parties when authorized. Unauthorized exposure of this information could violate state and federal laws and/or can adversely affect the University as a whole or in part, or the interests of individuals associated with the University. *Class 2* data may only be disclosed to a third party with the permission of the Data Owner.

   ii. If a file which would otherwise be considered *less sensitive but* contains an element that is *Confidential,* M*oderately Sensitive data,* the entire file is considered to be *Confidential,* M*oderately Sensitive* information.

c. ***Class 3 Confidential, Low Sensitivity***

   i. Data classified as Class 3 (Confidential, L*ow Sensitivity)* includes data that is not explicitly defined as *Class 1 or Class 2* data but that is regulated while posing a lower risk to the individual and to the University, such as student email address. This data may require permission to share and contract language for hosted solutions. This data is not intended to be shared without authorization. Class 3 data is distributed on a need-to-know basis between members of the University staff, IT systems, and specific third parties when authorized. Unauthorized exposure of this information could violate state and federal laws and/or can adversely affect the University as a whole or in part, or the interests of individuals associated with the University. *Class 3* data may only be disclosed to a third party with the permission of the Data Owner.

ii. If a file which would otherwise be considered *less sensitive but* contains an element that is *Confidential,* Low *Sensitivity,* then the entire file is considered to be *low sensitivity* confidential information.

d. ***Class 4 Public***

i. Data classified as *public* includes all data that are published and broadly available, including student directory information. The types of data classified as *public* should be as broad as possible. Anyone may access *public* data. Care should be taken to use all University information appropriately and to respect all applicable laws. Information that is subject to copyright must only be distributed with the permission of the copyright holder.

Classification Matrix

CNU ITS will develop and work with Data Owners to create a department or application specific classification matrix. For example, the matrix below classifies data into the appropriate categories. The matrix also accounts for the risk or exposure the University may be subjected to in the event of a disclosure of data to unauthorized parties.

Classification	**CLASS 1** Information that are restricted, with the highest Security\Privacy Requirements	**CLASS 2** Information that are confidential, with moderate security\privacy requirements	**CLASS 3** FERPA directory information and other confidential business information	**CLASS 4** Information that may have some minor sensitivity but are not regulated by laws and contracts; as well as public information
Examples	SSN Passport Driver's License Passport Health Insurance Gramm-Leach-Bliley Act (GLBA) Covered information (nonpublic personal information) Tuition payments and/or financial aid) containing personally identifiable information (PII) *Payment Card holder data (PCI-DSS) *Medical treatment/diagnoses and history (HIPPA/PHI) Presidential working papers	Grades and GPA Class schedule Class Roster Transcripts Student Conduct record	Internal business documents under NDA Internal intellectual property Some university financial data FERPA Directory Information may include: *Name * Date of birth * Photograph * Major field of study * Participation in officially recognized activities * Weight and height of athletic team members * Dates of attendance * Degrees, honors, and awards received * The most recent educational institution attended * Date Admitted * Degree sought	Enrollment numbers ready to be published Public reports or data
Risk	HIGH	HIGH	MEDIUM	LOW
Access	Authorized individuals with approved access	Authorized individuals with approved access	CNU employees and non-employees with a business	CNU affiliates and general public with a "need to know"

			“need to know”	

Data Storage Matrix

	Public Data (Class 4)	**Confidential Data** (Class 1 and Class 2)		**Restricted Data** (Class 1)			
Data Types	Public Data	FERPA	Confidential not covered by FERPA	PCI-DSS	HIPPA/PHI	PII	GLBA
Google Drive: An enterprise solution that allows users to store, share and edit files as part of Google Apps.	✓	🔑	🔑	✗	✗	🔑	🔑
Google Mail: An enterprise solution that allows users to send and receive email as part of Google Apps.	✓	🔐	🔐	✗	✗	🔐	🔐
ITS Network File Shares: Network drives only accessible via the CNU network and managed by ITS	✓	🔑	🔑	✗	✗	🔑	🔑
Laptop: University-owned laptops	✓	🔐	🔐	✗	✗	🔐	🔐
Portable Storage Devices: Thumb drives, portable hard drives or any other portable device that is capable of storing files	✓	✗	✗	✗	✗	✗	✗
Third-Party Cloud Hosted Systems:	✓	🔒	🔒	🔒	🔒	🔒	🔒

Legend

✓	**Use Permitted** There are no technical, policy or contractual issues that prohibit the sharing of this data type with appropriate intended users using this service. If you have questions about who you can share data with, contact the data owner.
🔑	**Use Permitted** in restricted folders with access limited to only CNU employees who have a need to know.
🔐	**Use Permitted** with approved methods of encryption.

🔒	**Use Restricted** Use of this service with the regulated data type is restricted and special approval is needed. Please contact the Information Security Officer at iso@cnu.edu for more information.
❌	**Use Prohibited** Use of this service with the regulated data type is prohibited. Do not use this service to send, store or share the regulated data type.

Definitions

Access: The ability to view information, and when permitted, update or download it.

Authorized Individual: An employee, consultant, volunteer or other individual who needs access to University information to perform an activity on behalf of the University. See also - System User.

Data: Information collected, stored, transferred or reported for any purpose, whether electronically or via hard copy.

Data Owner: As per the VITA Information Security Standard SEC 501, the data owner is the University manager responsible for the policy and practice decisions regarding data, including:

- Evaluating and classifying sensitivity of the data.
- Defining the protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.
- Communicating data protection requirements to the System Owner.
- Defining requirements for access to the data.

Data Custodian: As per the VITA Information Security Standard SEC 501, the data custodian is an individual who has been authorized to be in physical or logical possession of data by the Data Owner. The Data Custodian may also be a System Administrator.

- Protecting the data in their possession from unauthorized access, alteration, destruction, or usage.
- Establishing, monitoring, and operating IT systems in a manner consistent with COV Information Security policies and standards.
- Providing Data Owners with reports, when necessary and applicable.

Encryption: Encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information.

FERPA (Federal Education Rights and Privacy Act): The Family Educational Rights and Privacy Act (FERPA) is a federal privacy law that gives parents certain protections with regard

to their children's education records, such as report cards, transcripts, disciplinary records, contact and family information, and class schedules.

Gramm Leach Bliley Act (GLBA) Covered Information: GLBA covered information Christopher Newport University is required to protect covered customer data in accordance with the Gramm Leach Bliley Act (GLBA). This law applies to how higher education institutions collect, store, and use student financial records (e.g., records regarding tuition payments and/or financial aid) containing personally identifiable information. GLBA defines covered customer information as any record containing nonpublic personal information or personally identifiable financial information about a customer of CNU – whether in paper, electronic, or other form – that is handled or maintained by or on behalf of CNU or its affiliates.

- Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available
- Any information a student or other third party provides in order to obtain a financial service from CNU
- Any information about a student or other third party resulting from any transaction with CNU involving a financial service
- Any information otherwise obtained about a student or other third party in connection with providing a financial service to that person

A copy of this act can be obtained here: https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

HIPAA: Health Insurance Portability and Accountability Act, a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other healthcare providers.

PHI: Public Health Information, under the U.S. law is any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity, and can be linked to a specific individual. For example, medical records.

SEC 501: The Commonwealth of Virginia's Information Security Management Standard is often referred to as SEC 501. A copy of this document can be found at: https://www.vita.virginia.gov

SEC 525: The Commonwealth of Virginia's Hosted Environment Information Security Standard is often referred to as SEC 525. A copy of this document can be found at: https://www.vita.virginia.gov

System Administrator: The System Administrator is an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the System Owner, Data Owner, and/or Data Custodian. The System Administrator assists agency management in the day-to-day administration of agency IT systems, and implements security controls and other requirements of the agency information security program on IT systems for which the System Administrator has been assigned responsibility.

System Owner: The CNU business manager responsible for having an IT system operated and maintained. IT Systems may have only one System Owner. Example: The system owner for the online parking system would be the Director for Parking and Transportation Services. Responsibilities include:

- Require that the IT system users complete any system unique security training prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter.
- Manage system risk and developing any additional information security policies and procedures required to protect the system in a manner commensurate with risk.
- Maintain compliance with COV Information Security policies and standards in all IT system activities.
- Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.
- Designate a System Administrator for the system.

System Users: All users of University IT systems including, but not limited to, employees and contractors are responsible for the following:

- Reading and complying with agency information security program requirements.
- Reporting breaches of IT security, actual or suspected, to their agency management and/or the Information Security Officer (ISO).
- Taking reasonable and prudent steps to protect the security of University systems and data to which they have access.

University Data: Information collected, manipulated, stored, reported or presented in any format, on any medium, by any unit of the University.

References:

Information Security Policy - 6045

University Policy 6010: Acceptable Use of Computing Resources

University Policy 6035: Information Technology Change Management Policy

Data Access Standard

Data Protection Standard

Next Review Date: June 2024