CHRISTOPHER NEWPORT

UNIVERSITY

Data Protection Standard

VERSION 1.3

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**
October 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	1.1	Annual Review	Wendy Corrice
June 2021	1.1	Annual Review	Wendy Corrice
May 2022	1.2	Annual Review	Wendy Corrice
June 2023	1.3	Annual Review, added Scope, GLBA and definitions	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/GLBA/HIPPA) to secure access to data. Therefore, the University has developed the following procedures to meet the Commonwealth's Information Security Standards.

University data must be protected against threats such as malicious misuse, unauthorized intrusions, and/or inadvertent compromise. Activities conducted by off-campus entities must comply with the same security requirements as on campus entities. Each Christopher Newport University department and employee is responsible for the integrity and security of University data used, controlled, or accessed within their area. This standard establishes parameters for protection of University data, not the medium or application that the data resides in. This standard aligns with other established policies and procedures for data security in Institutional Research and the Commonwealth Security Standards.

Christopher Newport University collects and maintains restricted data about students, employees, donors, vendors, and others. This standard governs the use, control, and access to restricted data defined by statute, regulation, contract, license, or definitions within this standard.

Prior to use of restricted University data via laptop computer or other electronic portable data device, employees are responsible for obtaining appropriate protections for such computers or portable devices, or for verifying that such protections are already in place. The use of unprotected equipment to access or store University data is prohibited, whether or not the equipment is owned or controlled by the University, unless an exception has been granted by the Chief Information Officer (CIO) in writing.

Personal property is excluded from this standard provided that property does not in any manner make, access, store, or transport sensitive University information.

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.

General Security

In coordination with the Commonwealth Security Standards, ITS will develop appropriate specific procedures for compliance with this standard and provide education to the University community on the implementation of this standard and such procedures. Procedures, technology standards, and best practices can be found at the University’s policy website.

Restricted and internal University data must be saved to a University-owned, protected systems, except for rare instances that written approval is obtained from the Chief of Staff. Data Owners may request to store data on local machines through the CIO office, and the request will be forwarded to the Chief of Staff or appropriate data owner for approval. Access to saved and stored University data while on campus must be through the University network or provided services.

If the Chief of Staff grants permission for University data to be saved and stored on a non-University owned desktop, laptop or a personal device, faculty and staff are personally responsible for ensuring the data is encrypted to the same standards implemented by ITS on University owned systems. Faculty and staff are also responsible for deleting data at the conclusion of its approved use.

Employees are responsible for ensuring that appropriate security controls in accordance with published University standards are installed on their office and personal/home computers or any portable devices or media on which restricted University data is stored or accessed.

All University computers must have recommended operating system patches and updates installed, updated antivirus and antispyware tools installed, and firewalls turned on. Personal passwords are established and secured by employees. Passwords are not to be disclosed or shared.

ITS is responsible for the security of all Enterprise Information Systems throughout campus, including but not limited to, CNU Connect and associated systems, Active Directory, and the CNU e-mail system.

ITS will audit servers, computers, and portable devices or media with restricted data for compliance with policies and standards and will deny network access for servers, computers, and portable devices or media out of compliance.

Personal/Home Computers

Home computers that are used to access, store, or transmit restricted University data must use current security patches, updated antivirus and antispyware software, and encryption. It is imperative that appropriate approvals be pursued to use personal devices for University data storage or transmission. In instances where standard security precautions are not free, the user will incur all costs for security of their home computer. Employees are responsible for deleting all restricted University data from their computer upon termination of employment.

Remote Access

Remote access to restricted University data is available only to authorized users. Users must be authenticated to access restricted University data remotely. Data must be encrypted during transit. Access from off-campus internal must be via VPN and multifactored authentication provided by ITS.

Portable Devices or Media

Each user in the possession of restricted University data is responsible for protecting the data, regardless of the portable devices or media the data resides on.

Restricted University data may not be loaded onto any portable device or media unless protective measures are implemented that safeguard the confidentiality and integrity of the data in the event of theft or loss. Protective measures must be implemented before restricted University data is installed. Restricted University data cannot be saved and stored on mobile devices that cannot be encrypted with the current ITS standards.

Hosted / Service Providers (Off Campus)

Departments or faculty or staff who wish to engage an external provider are required to seek approval from the University CIO, ISO, and Chief of Staff prior to moving or copying University data. This requirement applies to all purchases regardless of the funding account used. Examples of hosted providers include but are not limited to:

- External Webhosting
- Cloud Hosting Services
- Any non-CNU organization

All hosted and service providers must provide computing and storage resources that reside only in the domestic United States as described in SEC525 (SI-2).

6. Equipment Disposal

University-owned computers and portable devices or media must have all confidential and official university data erased from the computer or portable device or media prior to its transfer out of University control, and/or destroyed, using current best practices referenced in the ITS surplus procedure.

International Travel

University faculty and staff should disclose to ITS via a Helpdesk work order that they will be traveling internationally. Faculty and staff should submit this work order with a minimum of **two (2) weeks notice**. University systems that are used to travel outside of the United States or its territories are required to receive a special configuration.

Enforcement

Failure to comply with current data security procedures may result in limiting or denying access to University data resources. If, upon investigation by the appropriate University officials, the lack of compliance appears to have been willful and deliberate or if there is repeated lack of compliance, disciplinary action may be taken.

Definitions

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: Programs and measures to encode information such that it cannot be decoded and read without knowing an appropriate key.

Enterprise Information System: Any centralized data storage or distribution system on campus. Enterprise Information Systems are managed by ITS.

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.

Internal/Limited Access University Data: Data that would not expose the University to loss if disclosed, but should be protected. Internal/limited access University data includes, but is not limited to, operational data likely to be distributed across organizational units within the University.

Network: Any number of computers and portable devices joined together by a physical or wireless communications link that allows information to be passed between computers, irrespective of where those computers are located. Networks provide the pathways for information traffic and allow employees to access databases and share applications residing on servers.

Personally Identifiable Information (PII): Data that can be used to uniquely identify an individual also defined in § 18.2-186.3.

Public University Data: Data available within the University community and to the general public.

Restricted University Data: Data protected by federal or state law or regulations, or by contract. Restricted University data includes, but is not limited to, data that is protected by the Family Educational Rights and Privacy Act (FERPA), or the Health Insurance Portability and Accountability Act (HIPAA).

SEC 501: The Commonwealth of Virginia's Information Security Management Standard is often referred to as SEC 501-9. A copy of this document can be found at: https://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501.pdf

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/media/vitavirginiagov/it-governance/psgs/pdf/HostedEnvironmentInformationSecurityStandardSEC52501.pdf

Server: An application or hardware that performs services for connected clients as part of a client server architecture.

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.

Next Review Date: June 2023