CHRISTOPHER NEWPORT

UNIVERSITY

Data Access Standard

VERSION 1.3

June 2023

Department: Information Security

Proprietary Statement

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 2021	1.1	Annual Review	Wendy L. Corrice
February 2022	1.2	Updated to remove version number from SEC501 references and updated System Administrator definition to match SEC501	Wendy Corrice
June 2023	1.3	Annual Review	Wendy L. 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.

Consistent with the University's obligation to preserve and protect information by all appropriate means, data will be made available to authorized individuals who have a valid business purpose for its use.

Violations of this procedure may lead to disciplinary action by the University up to and including dismissal from the University. Under certain circumstances, such violations may give rise to civil and/or criminal liability.

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.

Access to Data

The University determines levels of access to data and systems according to principles drawn from various sources such as federal and state law, University regulations, and ethical considerations. Individuals accessing University data and systems must observe requirements for confidentiality and privacy, must comply with protection and control procedures, and must accurately present the data in use. As per Commonwealth of Virginia's Information Security Management Standards, users will be required to successfully complete annual security awareness and compliance training to maintain access to University Systems. All University data must be protected in accordance with the University Data Protection Standard.

In accordance with Employee Separation Clearance Policy, supervisors are responsible for entering the separation date for the employee in the Employee Resource System to ensure prompt removal of access to all University Resources.

Upon approval by the appropriate university official, Information Technology Services (ITS) is responsible for maintaining procedures related to granting, modifying, and revoking access to Banner data and other enterprise managed systems. Modification of access to data is performed by ITS under the direction of the following University Officials / Offices.

Data	**University Official/Office**
Student Records Data	Registrar
Financial Aid Data	Director of Financial Aid
Admissions Data	Dean of Admission
Finance Data	University Comptroller
Alumni and Development Data	Vice President of Advancement

Departments that manage independent information systems housing university data, are required to submit their access control policies to the university ISO annually for certification.

Access to university data and systems is granted to individuals with whom the University has an active affiliation (e.g., students, faculty, staff, guests, vendors, etc.). Access may be granted or revoked in consultation with University management, and is not limited to the following situations:

- Situations that require immediate action to protect University data, systems, or individuals;
- Response to violations of University policies;

- Changes in employment responsibilities upon which access is no longer required;
- Termination of an individual's active affiliation with the University (e.g., employment termination, graduation, end of vendor contract, etc.).

In extreme circumstances, the ISO may take action to restrict access to protect the University.

Access to Banner data will be revoked on or before the date of employee termination specified by Human Resources or University Management. An exception to the removal of access may be granted to conduct University business for reasons such as, but not limited to coursework, grading, grade appeals, and research activities. ITS is responsible for documenting exceptions to the removal of access.

The University maintains data in a variety of databases and systems. Access to data is granted based on job responsibility and management's approval. After completing appropriate screening, data stewards may grant access data on a "need to know" basis. Frequently, the data accessed can be downloaded or exported to other applications such as desktop databases (i.e. Microsoft Access), spreadsheets, text, or hypertext. All individuals who are granted access to University data shall treat the data according to the same security and privacy rules in force within the system of origination regardless of where it is stored.

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 provided by ITS in accordance to the University VPN Policy.

Enforcement

Failure to comply with current data access 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

Access: The ability to view information, and, when applicable, 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 Users.

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.

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.

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.

Systems 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.

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

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 2024