CHRISTOPHER NEWPORT
UNIVERSITY

Security Awareness Training 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
April 2020	1.0	Standard Creation	Wendy L. Corrice
April 2021	1.0	Annual Review	Wendy Corrice
August 2021	1.1	Added Phishing Simulation Training	Wendy L. Corrice
June 2022	1.2	Annual Review Added Information Security Analyst Added VITA SEC501 and VITA SEC525 reference links	Wendy Corrice
June 2023	1.3	Annual Review Format update	Wendy Wilde

TABLE OF CONTENTS

Introduction

Christopher Newport University is committed to preserving the confidentiality, integrity, and availability of information technology assets, while preserving and nurturing the information-sharing requirements of academia. An important step in protecting the University's information assets is ensuring that all CNU personnel understand their roles and responsibilities in protecting University data.

Scope

Christopher Newport University Security Awareness Training Program applies to the following:

Faculty, Staff and Student Workers:

This standard applies to all faculty, staff and student workers as they may access, store, process, transmit or manage University data, systems, or applications. As members of the Christopher Newport University community faculty, staff and student workers are accountable, and have an obligation to demonstrate an understanding of their unique role and responsibility, as the best defense to ensure the protection of the University's information, data, and reputation.

Third Party Contractors (defined as vendors, consultants – non-Christopher Newport University employees) and Volunteers:

Third Party Contractors and volunteers who have access to University Data or systems in the course of their employment or volunteer activities are also covered by this standard. Third Party Contractors and volunteers are accountable and have an obligation to demonstrate an understanding of their unique role and responsibility as the best defense to ensure the protection of the University's information, data, and reputation.

Purpose

This standard defines the University's requirements for information security awareness training and education. Information Security Awareness Education is a new user and an annual requirement.

This standard is intended to meet the control requirements outlined in the VITA SEC501, Section 8.2 Security Awareness and Training Family Controls.

Roles and Responsibilities

1. **Data Owners** - 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:
    1. Evaluating and classifying sensitivity of the data.
    2. Defining the protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.
    3. Communicating data protection requirements to the System Owner.
    4. Defining requirements for access to the data.
2. **Information Security Officer (ISO)** - The Christopher Newport University employee, who is responsible for developing, enforcing and managing Christopher Newport University's information technology (IT) security program.
3. **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.
4. **System Owners** - The CNU business manager responsible for having an IT system (internal or hosted) 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:
    1. 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.
    2. Manage system risk and develop any additional information security policies and procedures required to protect the system in a manner commensurate with risk.
    3. Maintain compliance with COV Information Security policies and standards in all IT system activities.
    4. Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.
    5. Designate a System Administrator for the system.
5. **University Faculty, Staff, Student Workers and Volunteers** - All University-Related Persons are responsible for complying with this policy and, where appropriate, supporting and participating in processes related to compliance with this policy.
6. **Vice Presidents, Deans, Directors and Department Heads** - All Vice Presidents, Deans, Directors and Department Heads must take appropriate actions to comply with information technology and security policies. These individuals have ultimate

responsibility for University resources, for the support and implementation of this policy within their respective Units, and, when requested, for reporting on policy compliance to ISO.

Department heads or designees of department heads, are required to notify the ISO of new faculty, staff, student workers, consultants, volunteers or any other users requiring access to information technology resources so that these users can be assigned security awareness training accordingly.

Definitions

- **Availability** - The ability to make information and related physical and logical resources accessible as needed.
- **Confidentiality** - protecting information from being accessed by unauthorized individuals or applications.
- **Integrity -** is the trustworthiness and dependability of information. More specifically, it is the accuracy, consistency and reliability of the information content, processes and systems.
- **Insider threat** - An insider threat can happen when someone close to an organization with authorized access misuses that access to negatively impact the organization's critical information or systems.
- **Least Privilege** - The principle of least privilege is the idea that any user, program, or process should have only the bare minimum privileges necessary to perform its function.
- **Phishing** - the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information.

1. **Restricted System** - A restricted System is a term given to any IT system in which the classification is highly confidential according to Data Classification Standard.
2. **SEC 501** - The Commonwealth of Virginia's Information Security Management Standard is often referred to as SEC 501.

- **Social Engineering -** the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

1. **Third-Party Contractors** -defined as vendors or consultant(s), and not University employees.
2. **University Data** -University Data is any data or information that is created, owned, received, stored, or managed by Christopher Newport University.

Standard

CNU’s Security Awareness Training Standard and training program addresses roles, responsibilities, management commitment, coordination among organizational entities, and in compliance with the SEC501.

- **GENERAL SECURITY AWARENESS TRAINING**
    1. Security Awareness and Training content will be annually reviewed by the Information Security Officer and updated in response to compliance requirements and evolving security threats. Security Awareness and Training will include, at a minimum, contents described in the Information Security Standard (SEC501), such as the following.
    2. CNU’s Information Security Policies and Standards.
    3. The concept of separation of duties and least privilege.
    4. Prevention and detection of information security incidents, including those caused by malicious code.
    5. Proper disposal of data storage media.
    6. Proper use of encryption.
    7. Access controls, including creating and changing passwords and the need to keep them confidential.
    8. Phishing.
    9. Social engineering.
    10. Insider threat.
    11. Intellectual property rights, software licensing and copyright issues.

2. The ISO or designee will ensure that current versions of the Security policies and standards are included in the Security Awareness Training.
3. Each Department Head is responsible for ensuring that their respective employees, contractors and consultants complete mandatory Security Awareness Training.
4. The Information Security Officer, Information Security Analyst or designee may revoke account rights until mandatory Security Awareness Training is completed.

- **NEW USERS SECURITY AWARENESS TRAINING**

All new users must complete an initial Security Awareness Training course. This course may be conducted at Human Resource orientation, online or in person. New user information security awareness training must be completed within 30 days of account provisioning.

- **ANNUAL SECURITY AWARENESS TRAINING**

Beginning on July 1, 2020**,** all University faculty, staff, consultants, contractors and other designated users will be required to complete annual Security Awareness Training by December 31st of each calendar year following their initial hire security awareness training.

- **ROLE BASED SECURITY TRAINING**

Role-specific training will be provided to the following specialized users (System Owners, Data Owners, Data Custodians and System Administrators). Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. This training will also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security Programs. For detailed information, refer to the Role-Based Security Training Standard.

- **SECURITY TRAINING COMPONENTS**

A variety of methods will be employed to deliver Annual Security Awareness and Role-Based Security including, but not limited to:

1. Online Self-Paced Coursework.
2. Classroom Training.
3. Quarterly email Newsletters.
4. Information Security informational emails.
5. Incident Response training and tabletop exercises.
6. Phishing Simulation Training

- **ENFORCEMENT**

Failure to comply with this standard may result in denial or removal of access privileges to University information resources, without notice, and other disciplinary action up to and including termination.

- **TRAINING RECORD RETENTION**

To ensure compliance with the annual security awareness training, training will be documented and monitored by the Information Security Officer or designated person; and training records to support training activities will be retained for a minimum of three years in accordance with the Library of Virginia GS-103 requirements.

References:

Christopher Newport University Acceptable Use of Computing Resources (6010)

Christopher Newport University Unified Data Policy (6015)

Christopher Newport University Virtual Private Network Policy (6040)

Data Classification Standard

Data Encryption Standard

Remote Access and Virtual Private Network Standard

Role Based Security Training Standard

VITA SEC527 Security Awareness Training Standard

VITA SEC501 Information Security Standard

Next Review Date: June 2024