CHRISTOPHER NEWPORT
UNIVERSITY

Role Based Security 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
November 2017	1.0	Standard Creation	Nathan Bray
April 2020	1.1	Annual Review - Updated SEC501 links	Wendy Corrice
April 2021	1.1	Annual Review	Wendy Corrice
June 2022	1.2	Annual Review	Wendy Corrice
June 2023	1.3	Annual Review Added new departments Aligned the Roles and Responsibilities with the SEC501 Added the SEC525	Wendy Wilde

TABLE OF CONTENTS

Introduction

This standard defines an educational program that ensures requires that faculty and staff receive appropriate annual information security training based on their role in handling University data.

The Role Based Security Training (RBST) program complies with the AT-3 Security Training control, under SEC 501 and SEC 525, Recommended Security Controls for Commonwealth Information Systems and Organizations. The Information Security Officer (ISO) is responsible for tracking the compliance and oversight of the role based security training program.

Scope

The policy applies to specific roles the following University departments:

- Admission Office
- Advancement Office
- Auxiliary Services
- Business Office
- Counseling Services
- Financial Aid
- Honor Enrichment and Community Standards (CHECS)
- Human Resources
- Information Technology Services
- Physics, Computer Science and Engineering
- Police Department
- Registrar's Office
- Student Information Systems
- Residential Life
- Undergraduate Research and Create Activity

The RBST required by this policy is in addition to the University's required annual security awareness training. RBST is intended for staff members who maintain, operate or oversee the operation of information systems with restricted University data. This training program for Christopher Newport University meets the minimum guidelines specified in the **Commonwealth of Virginia's Information Security Management Standards (SEC 501 and SEC525)**.

Additional department roles not identified above may be added at the discretion of the Information Security Officer.

Procedures

Table 1 identifies the roles and corresponding annual Role Based Security Training (RBST)annual hourly training requirements.

Roles and Requirements

Table 1 – Minimum Annual RBST requirements

RBST Roles	CNU Job Titles/Roles	Relevant Responsibilities	Minimum Annual Training Requirements
System Owners	System Owner	The System Owner is the agency manager responsible for having an IT system operated and maintained. With respect to IT security, the System Owner's responsibilities include the following: 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 developing 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.	1 hour

		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. Note: Where more than one agency may own the IT system, and the agency or agencies cannot reach consensus on which should serve as System Owner, upon request, the CIO of the Commonwealth will determine the System Owner.	
Data Owner	All Designated Data Owners	The Data Owner is the agency manager responsible for the policy and practice decisions regarding data, and is responsible for the following: 1. Evaluate and classify sensitivity of the data. 2. Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs. 3. Communicate data protection requirements to the System Owner. 4. Define requirements for access to the data.	1 hour

Data Custodian	All Designated Data Custodians	Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following: 1. Protecting the data in their possession from unauthorized access, alteration, destruction, or usage. 2. Establishing, monitoring, and operating IT systems in a manner consistent with COV Information Security policies and standards. 3. Providing Data Owners with reports, when necessary and applicable.	1 hour

System Administrator	Information Technology (IT) Administrators, (e.g., network, system and database) Business Analyst Data Architect Developer Programmer System Architect System Engineer Software Engineer Test Engineer	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 hours

Security	Information Security Officer (ISO) All information security employees or contractors working for or contracted by the ISO	The ISO is responsible for developing and managing the agency's information security program. The ISO's duties are as follows: 1. Develop and manage an agency information security program that meets or exceeds the requirements of COV IT security policies and standards in a manner commensurate with risk. 2. Verify and validate that all agency IT systems and data are classified for sensitivity. 3. Develop and maintain an information security awareness and training program for agency staff, including contractors and IT service providers. Require that all IT system users complete required IT security awareness and training activities prior to, or as soon as practicable after, receiving access to any system, and no less than annually, thereafter. 4. Implement and maintain the appropriate balance of preventative, detective and corrective controls for agency IT systems commensurate with data sensitivity, risk and systems criticality. 5. Mitigate and report all IT security incidents in accordance with §2.2-603 of the Code of Virginia and VITA requirements and take appropriate actions to prevent recurrence. 6. Maintain liaison with the CISO. 7. Annually meet the requirements to obtain or maintain the Commonwealth ISO certification outlined in the link below: https://www.vita.virginia.gov/media/vitavirginiagov/commonwealth-	20 hours

		security/docs/COV-ISO-Certification-and-Continuing-Education-Requirements.pdf.	
Third Party Application Administrators	All Designated Third Party Application Administrators	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.	2 Hours

Table 2 identifies the crosswalk from the CNU Human Resources (HR) Job titles to the

RBST roles as well as the hourly pro-ration for employees who start their employment throughout the year.

Table 2 – Crosswalk of HR titles to RBST Roles

New Employee Proration Table

CNU Job Title/Role	RBST Role	Jan-Mar	Apr–June	July-Sept	Oct- Dec
Administrator	System/Software/Data	4	3	2	1
Architect	System/Software/Data	4	3	2	1
Business Analyst	System/Software/Data	4	3	2	1
ISO	ISO	20	15	10	5
Database	System/Software/Data	4	3	2	1
Developer	System/Software/Data	4	3	2	1
Engineer	System/Software/Data	4	3	2	1
System Owner	System Owner	1	1	1	1

Data Custodian/Data Owner	Data Custodian/Data Owner	1	1	1	1
Programmer	System/Software/Data	4	3	2	1
Project Manager	Manager	4	3	2	1
Information Security Analyst	Security	8	6	4	2
All others	N/A	N/A	N/A	N/A	N/A

Sources of RBST Training

The following sources may be used to complete the RBST requirement:

- Instructor led security training (internal and external)
- University provided security training (annual security, records management, etc.)
- Vendor security training (excludes sales presentations)
- Security related courses available in the Commonwealth Knowledge Center

Enforcement

Violations of this policy may lead to revocation of accounts or access to University data, without notice.

Definitions

SEC 501: The Commonwealth of Virginia's Information Security Management Standard is often referred to as SEC 501.

SEC 525: The Commonwealth of Virginia's Information Security Management Standard is often referred to as SEC 525.

Next Review Date: June 2024