CHRISTOPHER NEWPORT
UNIVERSITY

Account Management 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	Initial Plan	Wendy Corrice
June 2021	1.1	Annual Review	Wendy Corrice
June 2022	1.2	Annual Review	Wendy Corrice
June 2023	1.3	Annual Review	Wendy L. Wilde

TABLE OF CONTENTS

Introduction

User accounts control access to electronic resources. This document defines the standards for managing user accounts through their lifecycle to ensure individual accountability and based on the principle of least privilege.

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 SEC525) and Federal Law (FERPA/HIPPA) to secure access to data. Therefore, the University has developed the following standard to meet the Commonwealth's Information Security Standards.

Scope

This policy is applicable to those responsible for the management of user accounts, access to shared information or network devices. Such information can be held within a database, application or shared file space. This policy covers departmental accounts as well as those managed centrally.

Purpose

The purpose of this standard is to establish a standard for the administration of computing accounts that facilitate access or changes to Christopher Newport University data. An account, at minimum, consists of a user ID and a password; supplying account information will usually grant access to some set of services and resources. This standard establishes standards for issuing accounts, creating password values, and managing accounts.

Roles & Responsibilities

a. **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:
   i. Evaluating and classifying sensitivity of the data.
   ii. Defining the protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.
   iii. Communicating data protection requirements to the System Owner.
   iv. Defining requirements for access to the data.

b. **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.

c. **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.

d. **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:

i. 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.
ii. Manage system risk and develop any additional information security policies and procedures required to protect the system in a manner commensurate with risk.
iii. Maintain compliance with COV Information Security policies and standards in all IT system activities.
iv. Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.
v. Designate a System Administrator for the system.

Definitions

a. **Customer-facing Systems** include hardware, software or other technology with user interfaces or applications that directly interact with customers.

b. **Internal-facing Systems** include hardware, software or other technology used within the organization and are not exposed/available outside the organization.

c. **ADFS (Active Directory Federation Services)** - a software component developed by Microsoft, that runs on Windows Server operating systems to provide users with single sign-on access to systems and applications.

d. **Principle of "Least Privilege"** is a security concept promoting minimal user profile privileges on computers, based on users' job functions.

e. **Privileged Accounts** are accounts that provide elevated or non-restrictive access to the underlying platform that non-privileged user accounts do not.

f. **Sensitive System** - A Sensitive System is a term given to any IT system in which the classification is highly confidential according to Data Classification Standard

g. **Separation of Duties** - is the concept of having more than one person required to complete a task. In business the separation by sharing of more than one individual in one single task is an internal control intended to prevent fraud and error.

h. **Service Accounts** - privileged accounts that may not correspond to an actual person and are often built-in accounts that services use to access resources to perform activities. However, some system services require actual user accounts to perform certain functions.

Standard

Issuing Accounts

a. The owners of the system or designee shall make decisions regarding access to their respective data (e.g., the Registrar will determine who has access to registration data, and what kind of access each user has).

b. When issuing accounts, the standard security principles of "least privilege" and “separation of duties” to perform a function must be used. Accounts should not be granted any more privileges than those that are necessary for the functions the user will be performing. Access levels are to be associated with group or role membership, where practical, and all such IT system user accounts must belong to at least one user group.

c. A documented request to establish or modify an account on any IT system is required from the data owner or delegate. A user account must only be used by the person to whom it is assigned.

d. Unless required by regulatory requirements, accounts remain valid for the duration the individual maintains the relevant status within the University or until the account is closed or suspended by the University. Users are responsible for the lawful and appropriate use of information technology resources as described in the Acceptable Use Policy (6010).

e. The identity of users must be authenticated before providing account and password details. Authentication and authorization requirements are to be based on sensitivity and risk. The use of multi-factor authentication for remote access to sensitive IT systems is required.

f. No user is allowed to authorize their own access. Administrators who have access to add or elevate account privileges should have procedures in place for logging changes.

Passwords

a. Confirmation of the user's request for access credentials must be based on information already on file prior to delivery of the access credentials. Passwords for accounts must be delivered to users of all customer-facing IT systems securely. The use of non-shared, unique passwords on sensitive IT systems is required. Initial passwords must be changed upon first use unless the initial password was user selected using a secure method.

b. Automated password resets may be utilized, provided that a recognized and ISO approved method is used, such as multiple, random challenge and response questions. Password change events should be recorded in an audit log.

c. Password policies must comply with the SEC501 Security Standard: IA-5 Authenticator Management security controls and SEC525: Hosted Environment Information Security Standard.

d. Password policies for privileged user accounts are required to comply with complexity

requirements, and be changed every 42 days in compliance with the SEC501.

Managing Accounts

a. Processes to create, suspend, disable and terminate user and privileged accounts should be documented as well as approved by the System Owner or designee.

b. Department heads or supervisors should notify Human Resources and System Administrators in a timely manner about termination, transfer, or changes in access level requirements in accordance with the Employee Separation Clearance Policy (5080).

c. Unneeded accounts are to be disabled. Data in unneeded accounts in a disabled state shall be retained in accordance with the Library of Virginia and data owner requirements.

d. At least an annual review of all user accounts for sensitive IT systems is required to assess the continued need for the accounts access level and periodic review of user accounts for other IT systems. Annual review to be performed and documented by the Data Owner and reviewed by the ISO.

e. System Owners are responsible for documenting and implementing relevant security controls on their respective systems, such as password complexity and password change requirements. At least an annual review of security controls for sensitive systems shall be performed by the ISO or designee.

Privileged Accounts

Privileged accounts have a level of access above that of a normal user. Privileged access is typically granted to system administrators and staff performing computing account administration, or other such employees whose job duties require special privileges over a computing system or network. Individuals with privileged access must comply with applicable policies and IT standards.

a. Administrator Access:

Local administrator rights, or the equivalent on non-Microsoft Windows-based IT systems, should be granted only to authorized individuals.

b. Service Accounts:

Service accounts are a type of account necessary for systems to operate or interoperate. The ISO is responsible for designating and maintaining a list of individuals who have access to the account. The documentation should be available upon request for an audit or a security assessment.

c. System Administrator Accounts:

System administrator accounts perform super-user functions such as performing installs, altering critical system configurations or data, granting permissions to other accounts, etc. System

Administrators are required to have both an administrative account and at least one user account and are required to use their administrative accounts only when performing tasks that require administrative privileges. At least two individuals should have administrative accounts to each IT system, to provide continuity of operations.

System administrator accounts with remote access to sensitive systems, require multi-factor authentication for remote administration tasks.

Vendor-Consultant Accounts

Requests for vendor/consultant accounts to all sensitive systems must be documented according to standard practice and maintained on file. Documents must include access attributes for the account, be approved by the System Owner and communicated to the ISO. Accounts must automatically expire after a predetermined period.

Record Retention

As per the Library of Virginia (GS-113-000151) system access documentation will be retained for a minimum of three years after termination of user access.

Exceptions:

Exceptions to this standard will be handled in accordance with ITS security standards and with approval by the Chief Information Officer and/or Information Security Officer.

References:

VITA ITRM Information Security Standard (SEC501)
VITA SEC525: Hosted Environment Information Security Standard
Christopher Newport University Employee Separation Clearance Policy 5080
Virginia Department of Human Resource Management Policy 1.75 - Use of Electronic Communication and Social Media
Christopher Newport University Acceptable Use of Computing Resources Policy 6010
CNU Account Management Procedures
CNU Data Access Standard