CHRISTOPHER NEWPORT

UNIVERSITY

Encryption 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**
February 2020	1.0	Initial Release - All	Wendy L. Corrice
June 2021	1.1	Annual Review	Wendy L. Corrice
June 2022	1.2	Annual Review	Wendy L. Corrice
June 2023	1.3	Annual review and multiple updates. Aligned data classifications with Data Classification Standard, updated university owned on premise with “Restricted” data to Required, added Data Classification definitions	Wendy L. Wilde

TABLE OF CONTENTS

Purpose

The purpose of this compliance standard is to establish guidelines for the use of encryption to secure University information in transit on a network or stored on any form of media.

Scope

This document defines Information Technology Services (ITS) best practices for selecting and deploying encryption technologies and for the encryption of data. These procedures are intended to meet the control requirements outlined in the VITA SEC501 SC-28, Protection of Information at Rest and VITA SEC501 SC-13, Use of Cryptography.

Definitions

Class 1 Restricted:
Data classified as Class 1 (Restricted) may be subject to disclosure laws and warrant careful management and protection to ensure its integrity, appropriate access, and availability. This information must be guarded from disclosure. Unauthorized exposure of this information could contribute to identity theft, financial fraud, and violate state and/or federal laws. Unauthorized disclosure of this data could adversely affect the University, or the interests of individuals and organizations associated with the University. Systems containing restricted data must be approved by the Information Security Officer. Restricted data includes Social Security Number (SSN), Drivers License number, Federal ID, Health Insurance, Medical Record Number, Payment Card Holder Data, and Medical Information (PHI), when combined with identifying information.
Restricted data and systems should utilize measures such as encryption, two-factor authentication, or other added protections commensurate with the level of sensitivity and the compensating controls that are available. If a file which would otherwise be considered confidential contains any element of restricted data, the entire file is considered to be restricted information.

Class 2 Confidential, Moderate Sensitivity:
Data classified as Class 2 (Confidential, moderately sensitive) includes data that is not explicitly defined as restricted data but that is regulated and requires access control and contract language for hosted solutions. This data is not intended to be made publicly available or shared without authorization. Class 2 data is distributed on a need-to-know basis between members of the University staff, IT systems, and specific third parties when authorized. Unauthorized exposure of this information could violate state and federal laws and/or can adversely affect the University as a whole or in part, or the interests of individuals associated with the University. Class 2 data may only be disclosed to a third party with the permission of the Data Owner.
If a file which would otherwise be considered less sensitive but contains an element that is Confidential, Moderately Sensitive data, the entire file is considered to be Confidential, Moderately Sensitive information.

Class 3 Confidential, Low Sensitivity:
Data classified as Class 3 (Confidential, Low Sensitivity) includes data that is not explicitly defined as Class 1 or Class 2 data but that is regulated while posing a lower risk to the individual and to the University, such as student email address. This data may require permission to share and contract language for hosted solutions. This data is not intended to be shared without authorization. Class 3 data is distributed on a need-to-know basis between members of the University staff, IT systems, and specific third parties when authorized. Unauthorized

exposure of this information could violate state and federal laws and/or can adversely affect the University as a whole or in part, or the interests of individuals associated with the University. Class 3 data may only be disclosed to a third party with the permission of the Data Compliance Owner.
If a file which would otherwise be considered less sensitive but contains an element that is Confidential, Low Sensitivity, then the entire file is considered to be low sensitivity confidential information.

Class 4 Public:
Data classified as public includes all data that are published and broadly available, including student directory information. The types of data classified as public should be as broad as possible. Anyone may access public data. Care should be taken to use all University information appropriately and to respect all applicable laws. Information that is subject to copyright must only be distributed with the permission of the copyright holder.

Data at Rest: Defined as inactive data that is stored physically in any digital form.

Data in Transit: Defined as information that flows over the public or untrusted network such as the Internet and data that flows in the confines of a private network such as a corporate or enterprise Local Area Network (LAN).

Key: A key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm.

Mobile Device: Portable computing device that does not run standard Windows or macOS.

Off-Premise: Off-premise is a data resource that is installed in a remote facility or hosted in the cloud.

On-Premise: On-premise is a data resource that is installed on the premises of the person or organization using the software.

Methodology

Encryption should be considered as a protective control in situations where the risk associated with access to data at rest or in transit cannot be mitigated in other ways. Specifically, encryption should be leveraged in situations when there is a physical security risk to sensitive data or a logical security risk when transferring sensitive data through an untrusted network environment. However, since encryption typically reduces system/service performance, this should also be a consideration when designing the security approach. Overall, encryption must be carefully considered and selectively implemented.

Data at Rest Guidelines

For the following University-owned assets, IT Services has identified the specific areas where encryption is required and where staff should consider using encryption, but where it is not required.

University-owned end-user devices

Types of Systems	Operating system	Encryption Required	Encryption Recommended

Desktop	Windows		X
	macOS		X
Laptop	Windows	X	
	macOS	X	
Mobile device	Various	X	

University-owned servers

Location	**Data classification**	**Required**	**Recommended**
On-premise	Restricted	X	
	Confidential Moderate Sensitivity		X
	Confidential Low Sensitivity		X
	Public		X
Off-Premise	Restricted	X	
	Confidential Moderate Sensitivity	X	
	Confidential Low Sensitivity	X	
	Public		X

- Data Classification as defined by the Data Classification Standard :
    - Class 1: Restricted
    - Class 2: Confidential, Moderate Sensitivity

- Class 3: Confidential, Low Sensitivity
- Class 4: Public

Data in Transit Guidelines

Only encrypted connection methods are used to perform administrative functions on university systems.

Connection	Encryption Required	Encryption Recommended
HTTP (HTTP, HTTPS)	X	
FTP (FTP, SFTP, FTPS)	X	
SSH	X	
Remote Desktop	X	
VPN from off-campus	X	

Encryption outside of the United States: Note - users must comply with Federal law regarding the development and use of encryption outside of the United States.

Implementation Guidelines

Any large-scale encryption rollout will route through the University's change management process, which will ensure that encryption changes are documented, well-tested, and well-managed.

Key Storage

All centrally managed enterprise device encryption keystores are centrally stored and/or transmitted separately from the data being protected by the encryption key, managed, and retrievable as part of the University's backup process. Encryption keys and their backups must be retained for the lifetime of the data being protected

Exceptions:

Exceptions to this standard will be handled on a case by case basis and approval of the Information Security Officer.

References:

Information Security Policy - 6045

University Policy 6010: Acceptable Use of Computing Resources

University Policy 6035: Information Technology Change Management Policy

Data Access Standard

Data Classification Standard

Data Protection Standard

Review:

Next Review Date: June 2024