Compliance Component

Definition

Name	Cryptography
Description	Cryptography is the discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.
Rationale	Cryptography provides the necessary security features to protect unsecure data.
Benefits	• Client authentication • Data integrity • Confidentiality • User authentication • Non-repudiation

Associated Architecture Levels

Specify the Domain Name	Security
Specify the Discipline Name	Technology Controls
Specify the Technology Area Name	Cryptography

Compliance Component Type

Document the Compliance Component Type	Guideline
Component Sub-type	

Compliance Detail

State the Guideline, Standard or Legislation	The most commonly used encryption protocol is Transport Layer Security (TLS). HTTPS is Hypertext Transport Protocol integrated with TLS. TLS is sometimes referred to as TLS/SSL (Transport Layer Security/ Secure Socket Layer). Encryption should follow the latest standards in NIST and FIPS. Currently those standards are: • When transmitting sensitive or critical information over the web, users shall use encryption with at least: ○ Advanced Encryption Standard (AES) 256-bit encryption ○ Secure Hash Algorithim-2 (SHA-2) ○ Transport Layer Security 1.2 (TLS 1.2) • TLS 1.3 would be preferred if available. • Any ciphers used should be compatible with minimum TLS 1.2 ○ TLS 1.3 would be preferred if available. • Cryptography should be used for: ○ Email - Email is inherently unsecure. Cryptography allows the user to add a set of security features to email. ○ Stored Data - provides confidentiality and integrity of the data. It enables secure labeling, storing, and transferring of data.

	○ VPN - A public network such as the Internet accessed by a telephone line, cable or DSL, is inherently not secure. A VPN enables two or more parties to communicate securely across a public network by creating a private connection, or “tunnel,” between them. ○ Web Servers - Provides the necessary security features to protect the data on web servers that are unsecure. ○ Wireless Communication - There is a need for secure wireless access to networks where physical cables are not available and/or feasible. ○ Cloud – Authentication to cloud-provided systems and data. This document shall be reviewed annually or as needed.
Document Source Reference #	NIST Special Publications 800-52, Rev. 2 – *Guidelines for the Selection, Configuration and use of Transport Layer Security (TLS) Implementations*; IRS Publication 1075; NIST SP 800-53, Rev. 5 - *Security and Privacy Controls for Information Systems and Organizations* FIPS 140-3 – *Security Requirements for Cryptographic Modules*

Compliance Sources

Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC), IRS	*Website*	http://csrc.nist.gov
Contact Information	inquiries@nist.gov		
Name		*Website*	
Contact Information			

Keywords

List Keywords	TLS, HTTPS, FTP, SMTP, AES, Digital Signature, SHA-2, SSL, Cryptography, Web Server

Component Classification

Provide the Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*
Sunset Date				

Component Sub-Classification

Sub-Classification	Date	Additional Sub-Classification Information
☐ *Technology Watch*		
☐ *Variance*		
☐ *Conditional Use*		

Rationale for Component Classification

Document the Rationale for Component Classification	

Migration Strategy

Document the Migration Strategy	

Impact Position Statement

Document the Position Statement on Impact	

CURRENT STATUS

Provide the Current Status	☐ *In Development*	☒ *Under Review*	☐ *Approved*	☐ *Rejected*

AUDIT TRAIL

Creation Date	07/06/2023	*Date Approved / Rejected*	02/13/2025
Reason for Rejection			
Last Date Reviewed	01/28/2025	*Last Date Updated*	02/13/2025
Reason for Update	Vitality		