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). - When transmitting sensitive or critical information over the web, users shall use TLS with at least: - Advanced Encryption Standard (AES) 256-bit encryption - Secure Hash Algorithim-2 (SHA-2) - Transport Layer Security v 1.2 (TLS v 1.2) - Any ciphers used should be compatible with minimum TLS v 1.2. - 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.

	o Web Servers - Provides the necessary security features to protect the data on web servers that are unsecure.
	o Wireless Communication - There is a need for secure wireless access to networks where physical cables are not available and/or feasible.
	o Cloud – Authentication to cloud-provided systems and data.
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

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*	08/17/2023
Reason for Rejection			
Last Date Reviewed	07/27/2023	*Last Date Updated*	07/27/2023
Reason for Update	Vitality		