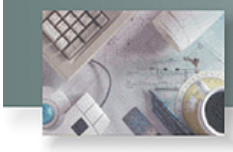

Compliance Component

DEFINITION	
Name	Hashing
Description	Hashing is the process of using an algorithm to encode information to ensure message integrity. Hashing makes it computationally infeasible to: 1. find a message that corresponds to a given hash output, or 2. find two different messages that produce the same output. Secure hashing is typically used in conjunction with other cryptographic algorithms.
Rationale	Hashing provides an additional layer of security to complement encryption.
Benefits	• Indicates to the recipient whether electronic information has or has not been modified during transmission. • Provides varying levels of confidentiality depending on the hash used.

ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Technical Controls
List the Technology Area Name	Cryptography
List Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	• The four approved algorithms for hashing are: o SHA-1 o SHA-256 o SHA-384 o SHA-512 • Hashing can be used for, but not limited to, protecting attachments in email, files being transferred and files in storage on various media.
Document Source Reference #	

Standard Organization			
Name	Federal Information Processing Standards Publication 180-2	*Website*	http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf
Contact Information			

Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
KEYWORDS			
List all Keywords			
COMPONENT CLASSIFICATION			
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Document the Rationale for Component Classification			
Conditional Use Restrictions			
Document the Conditional Use Restrictions			
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	04/13/2004	*Date Accepted / Rejected*	4/13/04
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			