COMPLIANCE COMPONENT

DEFINITION

Name	Data Integrity and Validation
Description	Data Integrity is the assurance that information is unchanged from its source, and has not been accidentally or maliciously modified, altered or destroyed. Validation is the tests and evaluations used to determine compliance with security specifications and requirements.
Rationale	Data integrity and validation minimize the risk to agency systems from malicious software and intrusions, or from accidental alteration or destruction.
Benefits	Data integrity addresses: • Protecting information from accidental or malicious alteration or destruction • Providing assurance that the information meets expectations about its quality • Providing assurance that the information has not been altered Validation: • Establishes compliance with security specifications and requirements

ASSOCIATED ARCHITECTURE LEVELS

Specify the Domain Name	Security
Specify the Discipline Name	Operational Controls
Specify the Technology Area Name	Data Integrity
Specify the Product Component Name	

COMPLIANCE COMPONENT TYPE

Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL

State the Guideline, Standard or Legislation	In computer systems, it is not always possible for humans to scan information to determine if data has been erased, added, or modified. Even if scanning were possible, the individual may have no way of knowing what the correct data should be. It is therefore desirable to have an automated means of detecting both intentional and unintentional modifications of data. • Data integrity - Reconciliation routines (e.g. checksums, hash totals, record counts) shall be used to ensure software or data has not been modified. • Data validation - Integrity verification programs (e.g. consistency and reasonableness checks, validation during data entry and processing) shall be used to look for evidence of data tampering, errors, and omissions. *NOTE: Refer to the Application Domain and Systems Management Domain.*
Document Source Reference #	

Compliance Sources

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

Keywords

List Keywords	Application, programming, software, system, reconciliation, verification, checksum, alteration

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	08/30/2007	*Date Approved / Rejected*	10/16/07
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			