DocuSign Envelope ID: E5CB13AF-9709-43DE-A395-44FC852E1C0C

North Carolina Department of Information Technology

Statewide Information Security Manual

January 2018

DocuSign Envelope ID: E5CB13AF-9709-43DE-A395-44FC852E1C0C

INTRODUCTION

PURPOSE

The purpose of this policy is to establish a statewide security policy for North Carolina State agencies and the State network. This policy also establishes principles to ensure a secure network infrastructure that integrates confidentiality, availability, and integrity into the infrastructure design, implementation, and maintenance, in order to do the following:

a. Protect the State's infrastructure and the citizen's data, whether hosted by external entities or within State data centers, from both internal and external threats.
b. Provide a consistent and repeatable framework for which IT assets can be securely connected to the State network.
c. Support the State's initiative to establish standards to manage technology, risks and increase consistency and accessibility.

OWNER

State Chief Risk Officer

SCOPE

The Statewide Information Security Manual is the foundation for information technology security in North Carolina. It sets out the statewide information security standards required by N.C.G.S. §143B-1376, which directs the State Chief Information Officer (State CIO) to establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the State's distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. These standards apply to all executive branch agencies, their agents or designees subject to Article 15 of N.C.G.S. §143B. Use by local governments, local education agencies (LEAs), community colleges, constituent institutions of the University of North Carolina (UNC) and other executive branch agencies is encouraged to the extent allowed by law.

POLICY

SECTION 1. ADOPTION OF NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) RISK MANAGEMENT FRAMEWORK SPECIAL PUBLICATION (SP) 800-37

The State has adopted the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 – *Guide for Applying Risk Management Framework (RMF) for Federal Information Systems,* as the standard for managing information security risk in State IT resources. The RMF provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. The NIST RMF utilizes NIST SP 800-53 as the foundation for identifying and implementing security controls. NIST 800-53 Rev 4 organizes these security controls into (17) Control Families. Table 1 identifies the control family names which will be utilized within the State security policies.

TABLE 1: SECURITY CONTROL FAMILY NAMES

DocuSign Envelope ID: E5CB13AF-9709-43DE-A395-44FC852E1C0C

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance		

SECURITY CATEGORIZATION

There are two levels of security categorization to be used within the State: ***Low*** and ***Moderate***. Security controls must be selected based on the data classification and security categorization of the information system and/or requirements for the specific operating environment.

> **Low Systems**: Systems that contain only data that is public by law or directly available to the public via such mechanisms as the Internet. In addition, desktops, laptops and supporting systems used by agencies are Low Risk unless they store, process, transfer or communicate Restricted or Highly Restricted data.
>
> **Moderate Systems**: Systems that stores, process, transfer or communicate Restricted or Highly Restricted data or has a direct dependency on a Moderate system. Any system that stores, processes, or transfers or communicates PII or other sensitive data types is classified as a Moderate system, at a minimum.

Agencies may tailor the baseline controls, as needed to enhance the security posture, based on their unique organizational needs. An example of such enhancement may occur due to additional requirements mandated by Federal agencies such as Internal Revenue Service (IRS) and other. All agencies are required to implement and comply with the baseline controls within the Statewide Information Security Manual, unless otherwise prescribed by Federal or State statute.

NIST SP 800-53 controls defines three types of controls:

- *Common Controls:* Those security controls that are Enterprise wide, e.g. State policies, Security devices provided by DIT, Enterprise email, etc. Agencies may inherit these controls as the system is managed outside of their authority. It is important to note that in order for a system to be considered **Inherited,** it must meet, at a minimum, the following criteria:
    - The system is managed by DIT, Cloud or other organizations outside the authority and security boundary of the agency
    - The State Chief Risk Officer has designated the control as inheritable
- *System-Specific Controls:* Those controls that provide security and other services for a particular information system only
- *Hybrid Controls:* Those controls which are shared between Enterprise, i.e. DIT, Cloud and/or Agency managed.

Agencies must evaluate each system and identify those that fall within the above listed control types. This step is crucial in facilitating and understanding roles and responsibilities as it pertains to audits and assessments. The following Table 2 - *Security Control Baseline* identifies those controls that will be implemented if a system is

DocuSign Envelope ID: E5CB13AF-9709-43DE-A395-44FC852E1C0C

categorized as Low or Moderate. The table is based on NIST 800-53 Rev 4 and has been modified to meet State of North Carolina use.

Note: Optional controls which have brackets, e.g. (X) are enhanced controls above the baseline requirement. Controls listed as "Optional" may be utilized to enhance the security posture of the information system. These controls are NOT to be considered mandatory. Agencies should understand that with the implementation of these controls may require additional funding. The description of these controls may be found at the following link: https://web.nvd.nist.gov/view/800-53/Rev4/home.

TABLE 2: SECURITY CONTROL BASELINES

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES	
		LOW	MOD
Access Control			
AC-1	Access Control Policy and Procedures	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	AC-3	AC-3
AC-4	Information Flow Enforcement	AC-4	AC-4
AC-5	Separation of Duties	AC-5	AC-5
AC-6	Least Privilege	AC-6	AC-6
AC-7	Unsuccessful Logon Attempts	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	Optional	Optional
AC-10	Concurrent Session Control	Optional	Optional
AC-11	Session Lock	AC-11	AC-11 (1)
AC-12	Session Termination	AC-12	AC-12
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14
AC-16	Security Attributes	Optional	Optional
AC-17	Remote Access	AC-17	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	AC-18	AC-18 (1)
AC-19	Access Control for Mobile Devices	AC-19	AC-19 (5)
AC-20	Use of External Information Systems	AC-20	AC-20 (1) (2)
AC-21	Information Sharing	Optional	AC-21
AC-22	Publicly Accessible Content	AC-22	AC-22
AC-23	Data Mining Protection	Optional	Optional
AC-24	Access Control Decisions	Optional	Optional
AC-25	Reference Monitor	Optional	Optional
Awareness and Training			
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1
AT-2	Security Awareness Training	AT-2	AT-2 (2)
AT-3	Role-Based Security Training	AT-3	AT-3
AT-4	Security Training Records	AT-4	AT-4
Audit and Accountability			
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1

DocuSign Envelope ID: E5CB13AF-9709-43DE-A395-44FC852E1C0C

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES	
		LOW	MOD
AU-2	Audit Events	AU-2	AU-2 (3)
AU-3	Content of Audit Records	AU-3	AU-3 (1)
AU-4	Audit Storage Capacity	AU-4	AU-4
AU-5	Response to Audit Processing Failures	AU-5	AU-5
AU-6	Audit Review, Analysis, and Reporting	AU-6	AU-6 (1) (3)
AU-7	Audit Reduction and Report Generation	Optional	AU-7
AU-8	Time Stamps	AU-8	AU-8 (1)
AU-9	Protection of Audit Information	AU-9	AU-9 (4)
AU-10	Non-repudiation	Optional	Optional
AU-11	Audit Record Retention	AU-11	AU-11
AU-12	Audit Generation	AU-12	AU-12
AU-13	Monitoring for Information Disclosure	Optional	Optional
AU-14	Session Audit	Optional	Optional
AU-15	Alternate Audit Capability	Optional	Optional
AU-16	Cross-Organizational Auditing	Optional	Optional
Security Assessment and Authorization			
CA-1	Security Assessment and Authorization Policies and Procedures	CA-1	CA-1
CA-2	Security Assessments	CA-2	CA-2 (1)
CA-3	System Interconnections	CA-3	CA-3 (5)
CA-4	Security Certification	Incorporated into CA-2.	Incorporated into CA-2.
CA-5	Plan of Action and Milestones	CA-5	CA-5
CA-6	Security Authorization	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7	CA-7 (1)
CA-8	Penetration Testing	Optional	Optional
CA-9	Internal System Connections	CA-9	CA-9
Configuration Management			
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (1) (3) (7)
CM-3	Configuration Change Control	CM-3	CM-3
CM-4	Security Impact Analysis	CM-4	CM-4
CM-5	Access Restrictions for Change	CM-5	CM-5
CM-6	Configuration Settings	CM-6	CM-6
CM-7	Least Functionality	CM-7	CM-7
CM-8	Information System Component Inventory	CM-8	CM-8 (3)
CM-9	Configuration Management Plan	CM-9	CM-9
CM-10	Software Usage Restrictions	CM-10	CM-10
CM-11	User-Installed Software	CM-11	CM-11
Contingency Planning			
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2
CP-3	Contingency Training	CP-3	CP-3

DocuSign Envelope ID: E5CB13AF-9709-43DE-A395-44FC852E1C0C

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES	
		LOW	MOD
CP-4	Contingency Plan Testing	CP-4	CP-4
CP-5	Contingency Plan Update	Incorporated into CP-2	Incorporated into CP-2
CP-6	Alternate Storage Site	Optional	CP-6 (1) (3)
CP-7	Alternate Processing Site	Optional	CP-7 (1) (2) (3)
CP-8	Telecommunications Services	Optional	CP-8
CP-9	Information System Backup	CP-9	CP-9 (1)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10
CP-11	Alternate Communications Protocols	Optional	Optional
CP-12	Safe Mode	Optional	Optional
CP-13	Alternative Security Mechanisms	Optional	Optional
Identification and Authentication			
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	IA-2	IA-2 (8)
IA-3	Device Identification and Authentication	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4
IA-5	Authenticator Management	IA-5	IA-5
IA-6	Authenticator Feedback	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	IA-8	IA-8
IA-9	Service Identification and Authentication	Optional	Optional
IA-10	Adaptive Identification and Authentication	Optional	Optional
IA-11	Re-authentication	Optional	Optional
Incident Response			
IR-1	Incident Response Policy and Procedures	IR-1	IR-1
IR-2	Incident Response Training	IR-2	IR-2
IR-3	Incident Response Testing	Optional	IR-3 (2)
IR-4	Incident Handling	IR-4	IR-4
IR-5	Incident Monitoring	IR-5	IR-5
IR-6	Incident Reporting	IR-6	IR-6
IR-7	Incident Response Assistance	IR-7	IR-7
IR-8	Incident Response Plan	IR-8	IR-8
IR-9	Information Spillage Response	Optional	Optional
IR-10	Integrated Information Security Analysis Team	Optional	Optional
Maintenance			
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1
MA-2	Controlled Maintenance	MA-2	MA-2
MA-3	Maintenance Tools	Optional	MA-3 (1) (2)
MA-4	Nonlocal Maintenance	MA-4	MA-4 (2)
MA-5	Maintenance Personnel	MA-5	MA-5

DocuSign Envelope ID: E5CB13AF-9709-43DE-A395-44FC852E1C0C

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES	
		LOW	MOD
MA-6	Timely Maintenance	Optional	MA-6
Media Protection			
MP-1	Media Protection Policy and Procedures	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2
MP-3	Media Marking	Optional	MP-3
MP-4	Media Storage	Optional	MP-4
MP-5	Media Transport	Optional	MP-5
MP-6	Media Sanitization	MP-6	MP-6
MP-7	Media Use	MP-7	MP-7 (1)
MP-8	Media Downgrading	Optional	Optional
Physical and Environmental Protection			
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2
PE-3	Physical Access Control	PE-3	PE-3
PE-4	Access Control for Transmission Medium	PE-4	PE-4
PE-5	Access Control for Output Devices	Optional	PE-5
PE-6	Monitoring Physical Access	PE-6	PE-6 (1)
PE-8	Visitor Access Records	PE-8	PE-8
PE-9	Power Equipment and Cabling	Optional	PE-9
PE-10	Emergency Shutoff	Optional	PE-10
PE-11	Emergency Power	Optional	PE-11
PE-12	Emergency Lighting	PE-12	PE-12
PE-13	Fire Protection	PE-13	PE-13 (3)
PE-14	Temperature and Humidity Controls	PE-14	PE-14
PE-15	Water Damage Protection	PE-15	PE-15
PE-16	Delivery and Removal	PE-16	PE-16
PE-17	Alternate Work Site	Optional	PE-17
PE-18	Location of Information System Components	Optional	PE-18
PE-19	Information Leakage	Optional	Optional
PE-20	Asset Monitoring and Tracking	Optional	Optional
Planning			
PL-1	Security Planning Policy and Procedures	Optional	PL-1
PL-2	System Security Plan	Optional	PL-2 (3)
PL-4	Rules of Behavior	PL-4	PL-4
PL-5	Privacy Impact Assessment	Optional	Incorporated in RA-3
PL-7	Security Concept of Operations	Optional	Optional
PL-8	Information Security Architecture	PL-8	PL-8
PL-9	Central Management	Optional	Optional
Personnel Security			
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1
PS-2	Position Risk Designation	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3

DocuSign Envelope ID: E5CB13AF-9709-43DE-A395-44FC852E1C0C

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES	
		LOW	MOD
PS-4	Personnel Termination	PS-4	PS-4
PS-5	Personnel Transfer	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8
Risk Assessment			
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3
RA-4	Risk Assessment Update	Incorporated into RA-3	Incorporated into RA-3
RA-5	Vulnerability Scanning	RA-5	RA-5 (1) (2) (5)
RA-6	Technical Surveillance Countermeasures Survey	Optional	Optional
System and Services Acquisition			
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2
SA-3	System Development Life Cycle	SA-3	SA-3
SA-4	Acquisition Process	SA-4 (10)	SA-4 (1) (2) (9) (10)
SA-5	Information System Documentation	SA-5	SA-5
SA-8	Security Engineering Principles	Optional	SA-8
SA-9	External Information System Services	SA-9	SA-9 (2)
SA-10	Developer Configuration Management	Optional	SA-10
SA-11	Developer Security Testing and Evaluation	Optional	SA-11
SA-12	Supply Chain Protection	Optional	Optional
SA-13	Trustworthiness	Optional	Optional
SA-14	Criticality Analysis	Optional	Optional
SA-15	Development Process, Standards, and Tools	Optional	Optional
SA-16	Developer-Provided Training	Optional	Optional
SA-17	Developer Security Architecture and Design	Optional	Optional
SA-18	Tamper Resistance and Detection	Optional	Optional
SA-19	Component Authenticity	Optional	Optional
SA-20	Customized Development of Critical Components	Optional	Optional
SA-21	Developer Screening	Optional	Optional
SA-22	Unsupported System Components	Optional	Optional
System and Communications Protection			
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1
SC-2	Application Partitioning	SC-2	SC-2
SC-3	Security Function Isolation	Optional	Optional
SC-4	Information in Shared Resources	Optional	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5

DocuSign Envelope ID: E5CB13AF-9709-43DE-A395-44FC852E1C0C

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES	
		LOW	MOD
SC-6	Resource Availability	Optional	Optional
SC-7	Boundary Protection	SC-7	SC-7
SC-8	Transmission Confidentiality and Integrity	SC-8	SC-8
SC-10	Network Disconnect	SC-10	SC-10
SC-11	Trusted Path	Optional	Optional
SC-12	Cryptographic Key Establishment and Management	SC-12	SC-12
SC-13	Cryptographic Protection	SC-13	SC-13
SC-15	Collaborative Computing Devices	SC-15	SC-15
SC-16	Transmission of Security Attributes	Optional	Optional
SC-17	Public Key Infrastructure Certificates	SC-17	SC-17
SC-18	Mobile Code	SC-18	SC-18
SC-19	Voice Over Internet Protocol	Optional	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	SC-21	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	SC-22	SC-22
SC-23	Session Authenticity	SC-23	SC-23
SC-24	Fail in Known State	Optional	Optional
SC-25	Thin Nodes	Optional	Optional
SC-26	Honeypots	Optional	Optional
SC-27	Platform-Independent Applications	Optional	Optional
SC-28	Protection of Information at Rest	Optional	SC-28
SC-29	Heterogeneity	Optional	Optional
SC-30	Concealment and Misdirection	Optional	Optional
SC-31	Covert Channel Analysis	Optional	Optional
SC-32	Information System Partitioning	Optional	Optional
SC-34	Non-Modifiable Executable Programs	Optional	Optional
SC-35	Honeyclients	Optional	Optional
SC-36	Distributed Processing and Storage	Optional	Optional
SC-37	Out-of-Band Channels	Optional	Optional
SC-38	Operations Security	Optional	Optional
SC-39	Process Isolation	Optional	Optional
SC-40	Wireless Link Protection	SC-40	SC-40
SC-41	Port and I/O Device Access	Optional	Optional
SC-42	Sensor Capability and Data	Optional	Optional
SC-43	Usage Restrictions	Optional	Optional
SC-44	Detonation Chambers	Optional	SC-44
System and Information Integrity			
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1
SI-2	Flaw Remediation	SI-2	SI-2 (2)
SI-3	Malicious Code Protection	SI-3	SI-3 (1) (2)

DocuSign Envelope ID: E5CB13AF-9709-43DE-A395-44FC852E1C0C

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES	
		LOW	MOD
SI-4	Information System Monitoring	SI-4	SI-4 (2) (4) (5)
SI-5	Security Alerts, Advisories, and Directives	SI-5	SI-5
SI-6	Security Function Verification	Optional	Optional
SI-7	Software, Firmware, and Information Integrity	Optional	SI-7 (1) (7)
SI-8	Spam Protection	Optional	SI-8 (1) (2)
SI-10	Information Input Validation	Optional	SI-10
SI-11	Error Handling	Optional	SI-11
SI-12	Information Handling and Retention	SI-12	SI-12
SI-13	Predictable Failure Prevention	Optional	Optional
SI-14	Non-Persistence	Optional	Optional
SI-15	Information Output Filtering	Optional	Optional
SI-16	Memory Protection	Optional	SI-16
SI-17	Fail-Safe Procedures	Optional	Optional

DocuSign Envelope ID: E5CB13AF-9709-43DE-A395-44FC852E1C0C

SECTION 2. IMPLEMENTATION AND MANAGEMENT

This Manual is the foundation for information technology security in state government and is required for all executive branch agencies to follow in order to comply with statewide information security standards. To be successful, Agency leadership must continue to emphasize the importance of information security throughout their organizations and at their discretion, implement additional supplementary controls as deemed necessary. When considering the supplementary controls not included in the State's policies, agencies should refer to NIST SP 800-53 Rev 4 and industry security practices related to information technology implementation. Agencies are also required to ensure ongoing compliance by implementing continuous monitoring activities.

SECTION 3 – INFORMATION PROTECTION

Agencies must implement appropriate safeguards as defined in the supporting policy documents (such as identification and authentication, encryption, data filtering, tagging, Multi-factor authentication or segregation) to ensure Restricted and Highly Restricted information, including Personally Identifiable Information (PII), Federal Tax Information (FTI), Payment Card Industry (PCI) is protected from inappropriate disclosure, misuse, or other security breaches, in accordance with State, Federal and other security standards and requirements.

Agencies must ensure an appropriate response in the event of a breach of sensitive PII consistent with Federal and Agency standards and requirements.

SECTION 4 – CONTINUOUS MONITORING

Continuous monitoring, automatic alerting, and auditing with corresponding tracking capabilities and reporting are required for devices connected to the State infrastructure or supporting State business (e.g. cloud services). Agencies must also have procedures in place to ensure robust incident response to unauthorized accesses and activities. The State CIO has the authority to require the installation of monitoring or auditing agents on devices connected to the network.

SECTION 5 – SECURITY ARCHITECTURE

Agencies must implement appropriate information safeguards (such as encryption, data filtering, tagging, or segregation) to ensure highly restricted information, including Personally Identifiable Information (PII), Federal Tax Information (FTI), Payment Card Industry (PCI) is protected from inappropriate disclosure, misuse, or other security breaches, in accordance with State, Federal and other security standards and requirements.

Agencies must ensure an appropriate response in the event of a breach of sensitive PII consistent with Federal and Agency standards and requirements.

SECTION 4 – REFERENCES

The following policies in the Statewide Information Security Manual provide additional details for the implementation of State information technology resources.

- SCIO-SEC-301: Access Control Policy (AC)
- SCIO-SEC-302: Awareness and Training Policy (AT)

DocuSign Envelope ID: E5CB13AF-9709-43DE-A395-44FC852E1C0C

- SCIO-SEC-303: Audit and Accountability Policy (AU)
- SCIO-SEC-304: Security Assessment and Authorization Policy (CA)
- SCIO-SEC-305: Configuration Management Policy (CM)
- SCIO-SEC-306: Contingency Planning Policy (CP)
- SCIO-SEC-307: Identification and Authentication Policy (IA)
- SCIO-SEC-308: Incident Response Policy (IR)
- SCIO-SEC-309: Maintenance Policy (MA)
- SCIO-SEC-310: Media Protection Policy (MP)
- SCIO-SEC-311: Personnel Security Policy (PS)
- SCIO-SEC-312: Security Planning Policy (PL)
- SCIO-SEC-313: Physical and Environmental Protection Policy (PE)
- SCIO-SEC-314: Risk Assessment Policy (RA)
- SCIO-SEC-315: System and Services Acquisition Policy (SA)
- SCIO-SEC-316: System and Communications Protection Policy (SC)
- SCIO-SEC-317: System and Information Integrity Policy (SI)