Assessment, Authorization and Monitoring Policy

Document No.
SCIO-SEC-304

Effective Date	**Review Date**	**Version**	**Page No.**
01/29/2018	03/26/2025	4	1 of 11

Scope

The Statewide Information Security Policies are the foundation for information technology security in North Carolina. The policies set 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. This policy covers all State information and information systems to include those used, managed, or operated by a contractor, an agency, or other organization on behalf of the State. This policy applies to all State employees, contractors, and all other users of State information and information systems that support the operation and assets of the State. 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. This security policy is consistent with applicable laws, executive orders, directives, regulations, other policies, standards, and guidelines.

This policy document provides the State of North Carolina's (State) security policy statements for the security assessment and authorization process for the effective and secure management of logical access to information systems and data of which the State is considered the owner.

Material Superseded

This current policy supersedes all previous versions of the policy. All State agencies and vendors of the State are expected to comply with the current implemented version of this policy.

Responsibilities

Covered personnel performing designated roles in the security assessment and authorization process are responsible that the processes are executed and maintained in compliance with State and local agency policies in order to ensure that access to information assets is appropriate to the job responsibilities of every individual interacting with State owned information assets.

Role	Definition
Agency Management	The Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designated organizational officials at the senior leadership level are assigned the responsibility for the continued development, dissemination, implementation, operation and monitoring of the Assessment and Authorization program.

Enterprise Security Risk Management Office (ESRMO)	The ESRMO is responsible for providing an enterprise approach to optimizing information technology (IT) security and risk management activities performed at the state and agency level.
Management	Management is responsible for documenting, tracking and reporting on the security state of agency information systems through the security authorization process. They may designate individuals to fulfill specific roles and responsibilities within the agency risk management process.
Assessment and Authorization Personnel	All covered personnel are responsible for assessing and or authorizing information system access must follow all State and local agency policies and procedures that are required for the effective implementation and assessment of selected controls and control enhancements in the security assessment and authorization process.

CA-1 – Policy and Procedures

All information assets that process, store, receive, transmit or otherwise could impact the confidentiality, integrity, and accessibility of State data must meet the required security controls defined in this policy document that are based on the National Institute of Standards and Technology (NIST) SP 800-53, Security and Privacy Controls. This document addresses the requirements set forth by the State to implement the family of Assessment, Authorization and Monitoring security controls at the organization, process and/or system level for all information assets / State data. The Assessment, Authorization and Monitoring process is implemented to ensure compliance with State information security policies and is critical to minimizing the threat of breaches. Security assessments are conducted to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Authorization is the process of accepting the residual risks associated with the continued operation of a system and granting approval to operate for a specified period of time.

Authorization to operate State information technology assets shall be controlled and managed to ensure that only authorized systems including workstations, servers, cloud computing applications, software applications, mobile devices, networks, and data repositories are implemented in accordance with an agency's business needs. It is the purpose of this policy to document the security assessment and authorization process for the State and its agencies to establish the necessary security best practices required to secure the State's information assets.

The State has adopted the Assessment, Authorization and Monitoring principles established in NIST SP 800-53 "Assessment, Authorization and Monitoring," control guidelines, as the official policy for this security domain. The "CA" designator identified in each control represents the NIST-specified identifier for the Assessment, Authorization and Monitoring control family. The following subsections in this document outline the Security Assessment and Authorization requirements that each State information system must implement and maintain to be compliant with this policy.

This policy and associated procedures shall be reviewed and updated annually, at a minimum. They shall also be updated following agency-defined events that necessitate such change.

This policy and the associated procedures shall be developed, documented, and disseminated by the Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designated organizational officials at the senior leadership level.

CA-2 - Control Assessments

Risk associated with each business system shall be assessed to determine what security requirements are applicable. Organizations shall select the appropriate assessor or assessment team for the type of assessment to be conducted. The control assessment determines the appropriate placement of each system and application within the security framework and evaluates the network resources, systems, data, and applications based upon their criticality. As the critical nature of the data and applications increases, the security measures required to protect the data and applications also increase. Control assessments must observe the following requirements:

1.1.1. Controls must be assessed under a Continuous Monitoring Plan supporting a frequency defined by the State Chief Information Security Officer (SCISO) for at least once every three (3) years, or when significant changes are made to the system or supported environment; and until the system is decommissioned.

1.1.2. The Continuous Monitoring plan shall be reviewed and approved by the State Chief Information Security Officer (SCISO) or designated representative prior to conducting the assessment.

a. Agencies shall provide to the State CIO their annual compliance and assessments reports, no later than September 1 of the given Calendar Year (CY). This certification includes compliance of cloud service providers. Any deficiencies identified within the agency which would preclude them from being compliant, must be addressed using the Corrective Action Plan (CAP) template. Reports must be submitted using approved secure methods.

b. Annual reports must ensure the agency has identified their security deficiencies and estimated cost for remediation. The report may include, but is not limited, to the following:

   i. Security boundary devices, e.g., firewalls, intrusion detection/prevention systems (IDPS)
   ii. Vulnerability management e.g., scanning, and patching systems
   iii. Resource constraints
   iv. Cybersecurity training deficiencies
   v. System development lifecycle (SDLC) deficiencies

d. When changes are made to an information system, a Security Impact Analysis shall be conducted to determine the extent to which changes to the information system will affect the security state of the system. These analyses are conducted as part of the System Development Lifecycle (SDLC) to ensure that security and privacy functional (and nonfunctional) requirements are identified and addressed during the development and testing of the system.

e. Agencies shall follow the procedures below when significant changes are made to the information system:

   i. Document assessment results and include correction or mitigation recommendations, to enable risk management and oversight activities.

   ii. Provide the assessment results to the ESRMO within thirty (30) days from the completion of the assessment.

   iii. The controls in the information system will be assessed on an annual basis to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system.

   iv. Cloud vendors must provide as an attestation of compliance via an independent third-party assessment report. Approved report types that meet the statewide requirement are provided in CA-7 of this policy. State agencies may include more restrictive requirements beyond the statewide requirement such as assessments that are performed against the Statewide Information Security Manual (SISM) and/or agency defined policies, standards, and other additional controls.

CA-2 (1) - Control Assessments | Independent Assessors

Third third-party assessors or assessment teams shall be employed to conduct control assessments. Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of information systems. Assessor independence provides a degree of impartiality to the process. To achieve impartiality, assessors should not do the following:

a. Create a mutual or conflicting interest with the organizations where the assessments are being conducted;

b. Assess their own work;

c. Act as management or employees of the organizations they are serving;

d. Place themselves in positions of advocacy for the organizations acquiring their services.

Independent assessments are typically contracted from public or private sector entities outside of the organization. This may include the NC National Guard Computer Network Defense (CND) Team.

CA-3 - Information Exchange

All information systems must use approved and managed information exchange from the information system to other information systems that do the following:

a. Information exchange using Interconnection Security Agreements (ISAs), business associate agreement (BAA), or service level agreement (SLA), etc.

b. As part of each exchange agreement, document the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, costs incurred under the agreement and the nature of the information communicated.

c. Employ deny-all and allow-by-exception policy for allowing systems that receive, process, store, or transmit data to connect to external information systems.

d. Monitor the information assets connections on an annual basis verifying enforcement of security requirements.

e. Follow the procedures below for connections to systems outside of the State Network:

   i. Establish an approved Memorandum of Understanding / Agreement (MOU/A) or Interconnection Security Agreement (ISA) signed by the State Chief Information Officer (SCIO) or designee or Agency CIO.

   ii. Submit a connection request as well as a Privacy Threshold Analysis (PTA) document to the Department of Information Technology (DIT). The request shall include the following:

      1. Type of connection to be established

      2. Type Connection requirements

      3. Key personnel to help coordinate the planning efforts of the system interconnection

      4. Duration of the interconnection

      5. Point of contact for the external organization requesting the interconnection of data and level of sensitivity of the data being exchanged.

   iii. Prior to system interconnection, system owners must complete a security impact analysis. The results must be provided to the Agency CIO for risk determination and approval.

   iv. Review and update ISAs at minimum annually or whenever there is a significant change to any of the interconnected systems.

   v. Terminate all interconnections when any of the following conditions are met:

      1. The ISA, MOU/MOA or SLA has expired or is withdrawn

2. The business requirement for the interconnection no longer exists
3. A significant change in the environment increases the risk to an unacceptable level of operations

Note: This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as website browsing.

CA-3 (5) - Information Exchange | Restrictions on External System Connections

All systems containing Restricted or Highly Restricted data shall have restrictions for connecting to external information systems. Organizations can constrain information system connectivity to external domains (e.g., websites) by employing deny-all, allow by exception policy, also known as whitelisting. Organizations determine what exceptions, if any, are acceptable.

CA-4 – Security Certification

Withdrawn: Incorporated into CA-2.

CA-5 – Plan of Action and Milestones/Corrective Action Plan

When deficiencies are discovered in the security posture of systems, a Plan of Action and Milestones (PO&AM) or Corrective Action Plan (CAP) shall be developed for such information systems that does the following:

a. Document the planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system.

b. Update existing action plans and milestones based on the findings from controls assessments, independent audit reviews, and continuous monitoring activities.

c. All discovered weaknesses, recommendations and their sources of discovery shall be traceable to the related CAP. Agency Security Liaisons shall review and validate completed CAPs to ensure that artifacts are in place supporting the closure, those CAPs not meeting criteria to close shall be returned to the security liaison for remediation and resubmission for closure.

d. The following information shall be included in each CAP:

   i. Type of weakness

   ii. Identity of the Agency, Division, Office responsible for resolving the weakness

iii. Estimated funding required for resolving the weakness

iv. Scheduled completion date for weakness remediation or mitigation

v. Key milestones with completion dates

vi. Source of weakness discovery

vii. Status of the corrective action, e.g., Ongoing or Completed

viii. Security Incidents

e. Identify and document any SCIO or delegate's decision to accept a weakness in a CAP.

f. CAPs must be reviewed and updated at minimum quarterly.

g. Identified weaknesses must be analyzed to determine level of risk, (e.g., high, medium, low)

h. Document weaknesses in an EGRC tool based on the following timelines:

i. Weaknesses identified as High must be entered if they cannot be remediated or mitigated within 30 days of discovery.

ii. Weaknesses identified as Medium must be entered if they cannot be remediated or mitigated within 60 days of discovery.

iii. Weaknesses identified as Low must be entered if they cannot be remediated or mitigated within 90 days of discovery.

iv. All remediated or mitigated weaknesses must have supported artifacts, e.g., screenshots, scan results etc.

CA-6 – Authorization

a. All information systems must have a senior-level executive (such as an Agency CIO or delegate), who is responsible for the information asset and authorizing the use of common controls available for inheritance by the information asset. The senior-level executive will ensure the following:

i. Ensure that the responsible individual accepts the use of common controls inherited by the system and authorizes the information asset for processing, e.g., Authority to Operate (ATO), before the system commences operations.

ii. Ensure the information system meets State, Federal and other mandates for compliance on an annual basis.

iii. Authorization levels shall be reviewed and updated regularly to prevent disclosure of information through unauthorized access.

b. All responsible parties shall consider whether granting authorization for an individual to use a system utility, (e.g., disk cleanup, disk defragmenter, system restore, disk compression and archival) may violate segregation of duties if the utility allows bypassing or overriding of segregation controls. If granting authorization to use a system utility could potentially violate segregation controls, the agency shall enact precautions to ensure that this violation does not occur. Detailed auditing or two-person control could provide assurance that segregation of duties is maintained. System utility misuse can cause the deletion or movement of files, the deletion of system restore points, or cause errors to occur in registry files.

c. System documentation and user procedures shall be updated to reflect changes based on the modification of applications, data structures and/or authorization processes.

d. Access shall require authentication and authorization to access needed resources, and access rights shall be regularly reviewed.

CA-7 – Continuous Monitoring

A program for system-level continuous monitoring and auditing of system use shall be implemented to detect unauthorized or unusual activity. The system-level continuous monitoring program should support the organization-level continuous monitoring strategy. This includes systems that are cloud hosted by contracted vendors or agency managed. All hardware connected to the State Network or cloud hosted shall be configured to support State/agency management and monitoring standards.

All organizations must complete an annual risk and security assessment of their critical systems and infrastructure and ensure that there are ongoing processes in place to assess the current posture of the environment. Continuous Monitoring is a program that ensures that all agencies are assessed annually at a minimum. The Continuous Monitoring program includes the following:

a. A configuration management process for the information system and its constituent components.

b. A determination of the security impact of changes to the information system and environment of operation.

c. Ongoing control assessments in accordance with the Continuous Monitoring Plan must include the following:

    i. Performance metrics concerning the status of control compliance and corrective actions required for identified control gaps;

    ii. Development of a process to evaluate supporting documentation;

    iii. The time required to monitor assessment recommendations;

iv. A schedule for assessing critical systems on an annual basis;

v. Security and Privacy status results reporting to be provided to ESRMO within 30 days of completion of an assessment through a corrective action plan (CAP);

vi. Coordination between the agencies and the ESRMO to address residual risks for those controls that cannot be implemented.

d. Business Owners and System Owners, in coordination with Agency CIOs, CISOs and Security Liaisons for State data residing in non-state locations, e.g., cloud or off-site hosted systems, shall ensure service providers do the following:

i. Agencies must ensure vendor compliance with Statewide security policies and obtain a Vendor Readiness Assessment Report (VRAR) from the vendor ***prior*** to contract approval.

ii. Implement the Continuous Monitoring Plan.

iii. For vendor hosted systems/solutions that will have Restricted or Highly Restricted data, agencies shall ensure that contract language requires vendors to provide as attestation to their compliance, an industry recognized, third party assessment report. Examples of acceptable attestation reports include Federal Risk and Authorization Management Program (FedRAMP) certification, Service Organization Controls (SOC 2) Type 2, ISO/IEC 27001:2022 Information Security Management Standard, and HITRUST CSF (Common Security Framework). In addition, vendors must provide the agency an industry recognized, third party assessment report annually for the duration of the contract.

Note: SaaS vendors cannot use IaaS/PaaS certifications unless the application is explicitly covered as part of those assessments.

iii. Correlate and analyze system level security-related information generated by assessments and monitoring to identify weaknesses and develop corrective actions.

iv. Report system level security and privacy status to the ESRMO through an EGRC repository, if available.

v. Demonstrate to the State that ongoing continuous monitoring activities are in place and compliance is being met for the following requirements:

1. Security
2. Privacy and Confidentiality
3. Availability (Business Continuity Management)
4. Processing integrity

CA-7 (1) – Continuous Monitoring | Independent Assessment

Third-party independent assessors or assessment teams shall be employed to monitor the controls in information systems on an ongoing basis. An independent 3rd party assessor is an entity separate from the agency and/or vendor that is being accessed and can provide an objective opinion on an information system. Organizations can maximize the value of assessments of system controls during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. Refer to CA-2 (1) - Control Assessments – Independent Assessors for more information.

CA-7 (4) Continuous Monitoring | Risk Monitoring

Risk monitoring is informed by the established organizational risk tolerance. Risk monitoring shall be an integral part of the continuous monitoring strategy / plan. The plan shall include the following:

a. Effectiveness monitoring, which determines the ongoing effectiveness of the implemented risk response measures.
b. Compliance monitoring, which verifies that required risk response measures are implemented. It also verifies that security and privacy requirements are satisfied.
c. Change monitoring, which identifies changes to organizational systems and environments of operation that may affect security and privacy risk.

CA-8 – Penetration Testing

All systems containing Restricted or Highly Restricted data shall have a penetration test performed by an independent third-party assessor at least annually. This may be part of a third-party assessment/certification, e.g., SOC 2 Type 2.

Endpoint threat monitoring of all devices shall be required including services within the cloud.

This control is optional for LOW risk information systems.

CA-9 – Internal System Connections

Security compliance checks must be performed between information systems and (separate) system components (e.g., intra-system connections) including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, internal connections for a class of components with common characteristics and/or configurations may be authorized, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration.

For enterprise solutions, DIT shall do the following:

a. Establish classes and subclasses of components permitted for internal system connections.

b. Develop baseline configurations for each component class and subclass.

c. Define interface characteristics and security and privacy standards for each component class and subclass connection type by FIPS-199 categorization – Moderate or Low.

d. Terminate internal system connections after agency-defined conditions.

e. Review the continued need for each internal connection on an agency-defined frequency.

Agency Business/System Owners shall only implement the established classes and sub-classes of components according to baseline configurations and security and privacy requirements. Any deviations from standards must be submitted through the DIT Exception Process.

Enforcement

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.