2025 SISM Revisions

Recommendation	Policy	Control	Description	Original Language	New/Revised Language
Revise header, e.g., logo, document number, etc., for all documents!	All	All			
Review and update Agency CIO, agency CIO, agency's CIO throughout all policies documents and make it consistent.	All	All			
Check bullets for accuracy, e.g., RA-3 had two bullet "f".	All	All			
Change signature on all policies from "Secretary of Department of Information Technology (DIT)" to North Carolina State Chief Information Officer	All		Change signature on all policies from "Secretary of Department of Information Technology (DIT)" to North Carolina State Chief Information Officer	Secretary of Department of Information Technology (DIT)	North Carolina State Chief Information Officer
Change State Chief Risk Officer (SCRO) to State Chief Information Security Officer (SCISO)	All	All	Change State Chief Risk Officer (SCRO) to State Chief Information Security Officer (SCISO)	State Chief Risk Officer (SCRO)	State Chief Information Security Officer (SCISO)
Add statement about exception process to SISM controls	SISM	Section 1: Security Categorization	Include statement in Statewide Information Security Manual document about NCDIT exception process and reference to process instructions.		Any deviations to required security controls must be submitted for approval through the DIT Exception Process.
Update physical access review to match IRS standards	Access Control	AC-1	Update physical access review to match IRS standards for physical areas that contain FTI/SSA data. Added IRS 1075 control references.	h.Documented review of employee badge/id card of general physical access annually and secure physical access quarterly. i.Documented review of non-employee/contractor badge/id card for both general and secure physical access quarterly.	h. Documented reviews shall be done for the following: i General Physical Access: - Employee Badge/ID Card – Annually - Non-employee/contractor/vendor Badge/ID card – Quarterly ii Secure Physical Access: - If access is given to secure physical area that contains FTI/SSA data, then the Badge/ID review to that secure physical area must be performed monthly regardless of employee type. See IRS 1075 Section 2.B.2 and 2.B.3.5 for more information. - If access is given to secure physical area that does NOT contain FTI/SSA data, then the Badge/ID review to that secure physical area must be performed quarterly regardless of employee type.
Add "do not" to inactivity time-out period statement	Access Control	AC-2 (5)	Statement should say "When users do not logout…" Add "See also NIST 800-63b section 4.3.3 Reauthentication"	When users logout, an inactivity time-out period of 15 minutes shall be implemented.	When users do not logout, an inactivity time-out period of 15 minutes shall be implemented. Individuals must physically log out or lock their device when they are expecting inactivity longer than the defined period of automatic enforcement of lockout (see AC-11). If there is someone in the vicinity of the user's system, while still logged on, there is risk of unauthorized individuals gaining access. See also NIST 800-63b section 4.3.3 Reauthentication.
Add "suspicious" to type of activity	Audit and Accountability	AU-2, AU-6	Change "unauthorized activity" to "unauthorized or unusual activity".	a. Implement a program for continuous monitoring and auditing of system use to detect unauthorized activity.	a. Implement a program for continuous monitoring and auditing of system use to detect unauthorized or unusual activity.
Change retention period from 3 years to 2 years.	Audit and Accountability	AU-4, AU-11	Change retention period for audit records from 3 years to 2 years.	Information systems shall retain audit records for at least three (3) years per the requirement stated in the NC Department of Natural and Cultural Resources State's General Schedule for State Agency Records, Information Technology Records.	Information systems shall retain audit records for at least two (2) years per the requirement stated in the NC Department of Natural and Cultural Resources State's General Schedule for State Agency Records, Information Technology Records.
Add "unusual" to type of activity"	Assessment, Authorization and Monitoring	CA-7	Change "unauthorized activity" to "unauthorized or unusual activity".	A program for system-level continuous monitoring and auditing of system use shall be implemented to detect unauthorized activity.	A program for system-level continuous monitoring and auditing of system use shall be implemented to detect unauthorized or unusual activity.
Update CA-7 to be in line with examples of 3rd party attestations.	Assessment, Authorization and Monitoring	CA-7	Modify CA-7(d)(iii) to match similar statements in RA-3 and SA-9.	iii. For vendor hosted systems/solutions that will have Restricted or Highly Restricted data, the agency must obtain one of the following independent third-party certifications from the vendor before contract award and receive one annually thereafter: 1. Federal Risk and Authorization Management Program (FedRAMP) 2. Service Organization Controls (SOC) 2 Type 2 3. ISO/IEC 27001 Information Security Management Standard 4. HITRUST CSF (Common Security Framework) Note: SaaS vendors cannot use IaaS/PaaS certifications unless the application is explicitly covered as part of those assessments.	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 to 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.
Expand/describe different types of monitoring for CA-7 (4).	Assessment, Authorization and Monitoring	CA-7 (4)	The control lists the different types of monitoring without explaining them.	Risk monitoring shall be an integral part of the continuous monitoring strategy / plan. The plan shall include the following: a. Effectiveness monitoring b. Compliance monitoring c. Change 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, identifies changes to organizational systems and environments of operation that may affect security and privacy risk.
Revise N-1 requirement and provide conditions for N-2.	Configuration Management	CM-2	Remove words "security related" from technologies. N or N-1 restriction should apply to all technologies. Also, revise N-1 requirement and provide conditions for N-2.	d: Ensure the baseline configuration of an information system is consistent with statewide enterprise architecture. Product versions of security related technologies must be either N or at N-1 and must be kept up to date by applying the latest security patches.	d. Ensure product versions of technologies are kept up to date and the latest security patches are applied. Agencies will ensure "best effort" to maintain all information technologies within N-1, where "N" is a major version. At minimum all operating systems and primary applications shall be maintained at baseline security configurations of no less than N-2. All current security patches for information technologies shall be applied prior to deployment and shall be maintained as meets or exceeds the SI-2 Flaw Remediation control. Whereas, "best effort" means taking, in good faith, all reasonable steps to achieve the objective, carrying the process to its logical conclusion and leaving no stone unturned.
Revise list of Application criticality categories	Contingency Planning	CP-2	Reorder list of criticality categories and change bullets to numbers to align with numbering schema within BCP application.	Application criticality has the following four categories (Definitions may be found in the Statewide Glossary of Information Technology Terms): •Statewide Critical •Department Critical •Program Critical •Noncritical	Application criticality has the following four categories (Definitions may be found in the Statewide Glossary of Information Technology Terms): i.Noncritical ii.Program Critical iii.Department/Agency Critical iv.Statewide Critical
Revise password management tools requirements	Identification and Authentication	IA-5	Provide additional requirements for the use of password management tools.	v. Agencies may use password management tools approved by the Enterprise Security and Risk Management Office (ESRMO). Approved password managers must be installed and managed locally on the user's machine (not offsite or in the "cloud"), must securely store passwords with a master key or key file, and must encrypt the password list with FIPS 140-2 encryption.	v. Agencies may use approved password management tools. Approved password managers must be installed and managed locally on the user's machine (not offsite or in the "cloud"), must securely store passwords with a master key or key file, and must encrypt the password list with FIPS 140-2 encryption (AES 256). In addition, agencies shall not use freeware solutions but rather purchase enterprise solutions. Also, agencies must create Standard Operating Procedures (SOPs) for the operations and management of such tools.
Update incident reporting website address.	Incident Response	IR-6	Update incident reporting website link and contact information.	ii. Use the incident reporting website https://it.nc.gov/cybersecurity-situation-report. iii. Contact a member of the ESRMO staff directly by phone or email security@its.nc.gov.	ii. Use the incident reporting website https://it.nc.gov/resources/cybersecurity-risk-management/statewide-cybersecurity-incident-report-form. iii. Contact a member of the DIT Threat Management staff directly by phone or email dit.threatmanagement@nc.gov.
Include requirement for third parties to provide to agency a verification of sanitized media.	Media Protection	MP-6	Third party entities that provide sanitization services must provide to agency documentation that media was sanitized when requested.		When an agency authorizes a third party or cloud vendor to destroy State data, all data shall be permanently deleted and shall not be recoverable, in accordance with NIST Special Publication 800-88 revision 1, and certificates of destruction shall be provided to the agency.

Remove/change bullets (c)(vii) and (c)(viii) concerning agencies using independent assessors for annual assessment.	Risk Assessment	RA-3	Remove/change bullets (c)(vii) and (c)(viii) concerning agencies using independent assessors for annual assessment. This is required every three (3) years, not annually.	vii. An agency may perform an annual self-assessment of their organization or system if they are storing, processing, or transmitting data that is classified as low or medium. An independent third-party assessment shall be completed every three years for systems storing, processing, or transmitting data classified as medium. viii. If an agency or system stores, processes, or transmits data classified as Highly Restricted, the agency shall use an independent assessor to conduct the annual assessment.	vii. An agency may perform an annual self-assessment of their organization or systems for two of the years out of a three year period. An independent third-party assessment shall be completed at least once every three (3) years.
Modify requirement about who is responsible for reviewing firewall changes	System and Communications Protection	SC-7	Modify requirement about who is responsible for reviewing firewall changes and how often.	Each firewall rule set shall be reviewed and verified by staff at least quarterly. If an outside entity, such as DIT, manages the firewall, then that entity shall be responsible for reviewing and verifying the firewall rule set at least quarterly.	Firewall rule implementation shall have an approval process that includes review by the Security Liaison, or designated personnel, of the agency that requires or no longer requires the rule. Existing firewall rules shall be reviewed every 6 months by the Security Liaison, or designated personnel, that is responsible for the application/device that requires the rule sets in question. For example, agency X application requires certain firewall rules to be implemented; therefore, that agency security liaison is responsible for approving and reviewing the firewall rules required for the application. Confirmation of the firewall rule review that is conducted every 6 months shall be sent to the ESRMO.
Revise SC-8 – Transmission Confidentiality and Integrity (I) regarding “supported” TLS versions.	System and Communications Protection	SC-8	Update TLS requirements regarding most current version to be used and disallowed versions.	All communications that transfer confidentially sensitive data between web clients and web servers must employ the most current secure transport protocol or at a minimum a supported version of TLS. Any TLS version that is no longer supported shall not be used.	All communications that transfer confidentially sensitive data between web clients and web servers must employ the most current secure transport protocol version(s) utilizing TLS as per NIST SP 800-52. Any TLS version that is disallowed, or not otherwise covered with a 'shall' and 'should' or has reached the end of a deprecation period as per NIST SP 800-52 shall not be utilized.
Revise State contact for vulnerability mitigation	System and Information Integrity	SI-2	Change contact from State Chief Risk Officer to State Chief Informaiton Officer to better align with statements throughout other policies.	x. When a “critical” or “high-level” risk vulnerability cannot be totally mitigated within the requisite time frame, agencies need to notify agency management and the State Chief Risk Officer (SCRO) of the condition and remediation plan and execution of a plan.	x. When a “critical” or “high-level” risk vulnerability cannot be totally mitigated within the requisite time frame, agencies need to notify agency management and the State Chief Information Security Officer of the condition and remediation plan and execution of a plan.
Add reference to CM-2 Baseline Configuration	System and Service Acquisition	SA-3	Add reference to CM-2 Baseline Configuration	f. The organization will plan for End-of-Life (EoL) and End-of-Support dates (EoS) for systems and services. This will ensure that systems and services can receive security patches and updates throughout the system development lifecycle, and that the organization is prepared to discontinue the system or service once no longer supported, or when security cannot be ensured.	f. The organization will plan for End-of-Life (EoL) and End-of-Support dates (EoS) for systems and services. This will ensure that systems and services can receive security patches and updates throughout the system development lifecycle, and that the organization is prepared to discontinue the system or service once no longer supported, or when security cannot be ensured. See also CM-2 Baseline Configuration for more information about supported versions of products.
Add "independent" to third-party risk assessment, and change "state statute" to "state policy".	System and Service Acquisition	SA-9	Add "independent" to third-party risk assessment, and change "state statute" to "state policy".	j. Contracts with vendors providing offsite hosting or cloud services that will host Restricted or Highly Restricted data must require the vendor to provide the State a third-party risk assessment report (e.g., Service Organization Control (SOC) 2 Type II, International Organization for Standardization (ISO) 27001, Federal Risk and Authorization Management Program (FedRAMP) Moderate), or HITRUST CSF (Common Security Framework) before contract award and annually thereafter to establish compliance with state statutes.	j. Contracts with vendors providing offsite hosting or cloud services that will host Restricted or Highly Restricted data must require the vendor to provide the State an independent, third-party risk assessment report (e.g., Service Organization Control (SOC) 2 Type II, International Organization for Standardization (ISO) 27001, Federal Risk and Authorization Management Program (FedRAMP) Moderate), or HITRUST CSF (Common Security Framework)) before contract award and annually thereafter to establish compliance with state policy.