2020 Statewide Information Security Manual Updates

Revision	Policy	Section	Description	New/Revised Language
Add Review Date to each policy document	All	Header	Add Review Date for last review date of policy.	Review Date
Remove "Agencies shall" from policy statements	All	All	Rename all statements so that requirements can apply to any entity (agency, third-party, etc.).	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.
Add section and language that current policy "supercedes" previous ones	All	Material Superseded	Add Material Superceded section to the end of each policy document.	Material Superseded: This current policy supersedes all previous versions of the policy.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.
Remove "where feasible"	All	All	Replaced instances of "where feasible" and "where possible" to "technically configurable", or simiar wording.	
Modify statement referencing NIST 800-53	All	xx-1	Change statement referencing NIST 800-53	All agency information assets must meet the required security controls defined in this policy document that are based on the NIST SP 800-53, Security and Privacy Controls.
Remove references to NIST 800-53 "Rev. 4"	All	xx-1	Remove "Rev. 4" from NIST 800-53 references.	
Remove "procedures" from policy opening statement	All	xx-1	Change "procedures" from statement about procedures and standards to "control".	
Rewrite statement about privileged access	Access Control	AC-2	Changed definition of privileged access.	Privileged accounts are accounts with elevated access and/or agency-defined roles assigned to individuals that allow those individuals to perform certain functions that ordinary users of that system are not authorized to perform.
Remove "smaller agencies"	Access Control	AC-5	Removed statement about "smaller agencies" and "the principle should be applied to the extent possible."	
Add optional logon banner for devices with limited display	Access Control	AC-8	Add an optional login banner for systems that cannot accommodate the standard logon banner.	This system is property of the State of North Carolina & is for authorized users ONLY. Unauthorized access may result in disciplinary action, civil & criminal penalties. Users have no expectation of privacy. USER EXPRESSLY CONSENTS TO MONITORING.
Update NSA configuration guide link	Configuration Management	CM-6	Update the following link: http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml	New link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/index.cfm
Modify application criticality categories	Contingency Planning	CP-2	Add language that requires DR for Statewide Critical and Department Critical	Agencies with Statewide and Departmental Critical systems must provide disaster recovery capabilities to ensure timely recover and restoration of service as part of their disaster recovery strategy.
Modify definition for MTD	Contingency Planning	CP-2	Modify Maximum Tolerable Downime (MTD)	The amount of time mission/business process can be disrupted without causing significant harm to the organization's mission
Modify contingency plan testing requirements	Contingency Planning	CP-4		Develop test objectives and success criteria to enable an adequate assessment of the Disaster Recovery and/or Restoration procedures. - Develop a contingency plan exercise after action report.
Require DR for Statewide and Department Critical	Contingency Planning	CP-10	Add statement that Statewide and Department critical sysems must have DR support.	Applications categorized as Statewide and or Department critical are recommended to have viable disaster recovery support, approval, budget in place, and be exercised according to policy.
Update NIST reference	Risk Assessment	RA-2	Correct NIST reference to be NIST 800-60.	
Update risk assessment scope	Risk Assessment	RA-3		Risk assessments takes into account risks posed to State agency operations and assets, or individuals from external parties, including but not limited to entities such as Service providers; Contractors operating information systems on behalf of the Agency; Individuals accessing State data and information systems; and Outsourcing organizations
Updated references to EGRC reporting tool	Risk Assessment, Security Assessment and Authorization	RA-3, CA-2 CA-5, CA-7	Change references to "DIT Enterprise Governance Risk Compliance (EGRC) reporting and tracking tool." to "a corrective action plan (CAP)."	
Update Appendix A	Risk Assessment	Appendix	Added revised template	
Add VRAR requirement for vendors	Risk Assessment	RA-3, CA-7 SA-4, SA-9	Add VRAR requirement statement	Agencies must ensure vendor compliance with Statewide security policies and obtain a Vendor Readiness Assessment Report (VRAR) from the vendor prior to contract approval. This requirement is for both solutions hosted on State infrastructure and those that are not hosted on State infrastructure.

Rename periodic scanning to real-time scanning	Risk Assessment	RA-5	Modify statement to be "real-time scanning".	Real-time scanning for spyware, adware and bots (software robots) with one or more anti-spyware programs that detect these malicious programs and help inoculate the system against infection
Replace "near future" with "established timeframe"	Risk Assessment	RA-5	Replace "near future" with "established timeframe"	
Update vulnerability risk ratings to be more adaptive and include additional information. Copy RA-5 to SI-2	Risk Assessment, System and Information Integrity	RA-5, SI-2		Where technically configurable, risk ratings shall be calculated based on active exploit threat, exploit availability, factors from the Common Vulnerability Scoring System (CVSS), and system exposure utilizing a scale of 0 to 10.0 as per the CVSS v3 “Qualitative Severity Rating Scale” for proper prioritization. If the additional combined information above is not available then the CVSS score, exploitability information, or a vendor rating where appropriate risk is reflected may be used. For general vulnerabilities that do not easily relate back to a CVE, such as unsupported software or encryption versions less than policy requirements, a vulnerability scanner rating that is above “info”, or a score of 0, may be used after appropriate review.
Add badges shall be visibly displayed at all times	Physical and Environmental Protection	PE-2	Added language based on OSHR requirement for displaying badges.	Everyone within a State building must display either a State Identification (ID) Badge or a numbered and current visitor badge. These badges are the property of the State and are provided to employees and visitors as a convenience. Badges must always be visible.
Updated reference to State Human Resources Manual	Personnel Security	PS-2, PS-3 PS-8	Update references and remove links to State Human Resources Manual. Replace text with the following: "policies published by the NC Office of State Human Resources (OSHR)."	
Update PII data classification section	Media Protection	MP-3	Added PII classification table regarding combining identifying information. Added disclaimer that this is not exhaustive.	
Reword Application Partitioning section	System and Communications Protection	SC-2	Reword statement on Special Assembly zone.	Systems not able to adhere to the DMZ and/or other security requirements of this policy need to be in a Special Assembly zone. Agencies must document the rationale for developing the a Special Assembly zone.
Change firewall policy review	System and Communications Protection	SC-7	Change "firewall policy" to "firewall rule set"	
Add language about extending network services	System and Communications Protection	SC-8	Add statement about agencies prohibiting the extending, modifying or retransmitting network services.	Agencies shall protect the confidentiality of data transmitted on the network from corruption or data loss by prohibiting the extending, modifying or retransmitting network services, such as through the installation of new switches or other network devices, unless prior agency CIO or delegate approval is granted.
Remove SSL	System and Communications Protection	SC-23	Remove SSL from list of mechanisms for session authenticity. Look at others!	
Modify encryption requirement for Information at Rest	System and Communications Protection	SC-28	Remove "on deployed workstations" and "exception when no apporved encryption technology…"	Restricted and Highly Restricted data stored in non-volatile storage (i.e. disk drive) on all endpoints shall be encrypted with FIPS 140-2 compliant encryption during storage (regardless of location).
Add description that this is a lab/test area	System and Communications Protection	SC-44	Add description that this is a lab/test area	Agencies tasked with conducting incident response and forensics, should employ a detonation chamber capability also known as dynamic execution environments in a secure, quarantined environment, to do the following:
Update incident response reporting for vendors	Incident Reponse	IR-6	Updated statement regarding timeframe for incident reporting.	Agencies and vendors of the State shall ensure all suspected security incidents or security breaches are reported to the ESRMO within twenty-four (24) hours of incident confirmation, as required by NC general statute. Incidents Incidents shall be reported to the ESRMO by one of the following methods:
Add requirement for security PoC in contracts	Incident Reponse	IR-6		Contracts involving the storage and/or processing of State data shall identify the vendor’s security point of contact (PoC).
Make Penetration Testing mandatory	Security Assessment & Authorization	CA-8	Modified penetration testing requirement to be mandatory to match continuous monitoring requirement	All systems containing Restricted or Highly Restricted data shall have a penetration test performed by an independent third-party assessor at least annually. Endpoint threat monitoring of all devices shall be required including services within the cloud. This control is optional for LOW risk information systems.

Add Threat Monitoring for cloud services as a requirement	System & Information Integrity	SI-4, CA-7		Agencies shall implement a program for continuous monitoring and auditing of system use to detect unauthorized activity. 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.
Remove "contribute to outside-party attack"	System & Information Integrity	SI-4	Statement is not needed anymore.	
Update firewall audit requirements	System & Information Integrity	SI-4(4)	Updated firewall audit requirements	b. Agencies shall enable logging features on firewalls, (network and web application firewalls (WAF)), to capture all packets dropped or denied by the firewall. Agencies shall review those logs at least monthly c. Agencies shall review and verify their firewall policies at least quarterly. If an outside entity, such as DIT, manages the firewall, then that entity shall be responsible for providing the agency's firewall policy to the responsible agency for review and corrective actions, at minimum quarterly.
Update verbiage to include the use of WAF	System & Information Integrity	SI-4(5)	Add "Web Application Firewalls (WAF)" as an example.	
Update Automatic Email Forwarding section	System and Information Integrity	SI-8	Modify language to restrict forwarding of state date to non-state emails.	Forwarding and auto-forwarding of state data must be in compliance with the Statewide Acceptable Use Policy (AUP).
Move email forwarding and retention requirements to SI-12	System & Information Integrity	SI-8, SI-12	Move email forwarding and retention requirements to SI-12	Agencies shall develop policies to encourage due care by users when forwarding electronic messages so that users do not do the following: a. Auto-forward email without first obtaining appropriate agency approval. The forwarding or auto-forwarding of state emails and/or state data to non-state email accounts is prohibited. b. Knowingly send out an email message that contains viruses, Trojan horses or other malware. c. Use the electronic-mail system or network resources to propagate chain letters, misinformation or hoax information. d. Forward any restricted or highly restricted information to any unauthorized party without prior management approval, and without appropriate protections, such as encryption. e. Forward the wrong attachment. f. Send information or files that can cause damage to the State of North Carolina or its citizens. g. Send unsolicited messages to large groups of people except as required to conduct agency business. Communications sent or received by agency email systems and/or email communications on State business in personal email accounts may be public records as defined by the North Carolina Public Records Law, N.C.G.S. §132.1, et seq., and shall be managed according to the requirements of an agency's record retention policy or as set forth in the General Schedule for Electronic Records published by the Department of Cultural and Natural Resources.