Policy Area: Information Security Program Charter	**Title:** Information Technology Security Program Charter for the North Carolina State Chief Information Officer (State CIO) and the Enterprise Security and Risk Management Office (ESRMO).

In North Carolina state government, state laws set the information technology security requirements and form the Information Security Charter. The matrix below lists those statutes, which define the roles and responsibilities for information technology security, risk and business continuity management and the compliance procedures that fulfill the legislative mandate.

Section	Statement	Compliance Procedures
147-33.76(b)(1)	*The State CIO shall be responsible for developing and administering a comprehensive long-range plan to ensure the proper management of the State's information technology resources. The State CIO shall set technical standards for information technology.... establish information technology security standards .... The State CIO is authorized to adopt rules to implement this article.*	The State CIO through the Enterprise Security and Risk Management Office (ESRMO) initiates proposed security policies and standards and reviews those recommended by others. Policies and standards are based on best practices and industry standards including ISO and NIST.
147-33.82(a)(3)	*The Office of Information Technology Services shall "[C]onduct an annual assessment of State agencies for compliance with statewide policies for information technology."*	The ESRMO continuously monitors agency compliance with statewide policies for information technology through a variety of measures, including reports of security incidents, questions and feedback from agencies and the annual update of the security manual.
147-33.110	*The State Chief Information Officer shall 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 communications and encryption technologies.*	The State Security Manual is published on the State CIO web site by the IT Policy and program section. After review by the ESRMO, draft security policies and standards are reviewed by the Policy and Legislative Section in the State CIO's Office. The proposed policies and standards are then circulated to the agencies for review and comment, including input from the agency security liaisons, agency CIO's and interested parties. When approved by the State CIO,

Section	Statement	Compliance Procedures
		policies and standards that do not contain confidential information are published on the State CIO's web site. The web site contains the Statewide Information Security Manual and other materials, including a glossary. The ESRMO operates the NC-ISAC including the Security Portal that provides information technology security alerts and notices to agencies. Agency procedures and practices are the means through which the statewide standards and policies are implemented.
147-33.110	*The State CIO shall review and revise the security standards annually. As part of this function, the State Chief Information Officer shall review periodically existing security standards and practices in place among the various State agencies to determine whether those standards and practices meet statewide security and encryption requirements.*	Statewide security standards are reviewed at least annually and updated as necessary. As requested by the State CIO, the ESRMO may review security standards and practices for other agencies. ESRMO coordinates the security standards deviation process to track remediation of reported non-compliance risks for the State CIO. Security standards compliance assessments are conducted and used to evaluate agency compliance with security policies and requirements.
147-33.110	*The State Chief Information Officer may assume the direct responsibility of providing for the information technology security of any State agency that fails to adhere to securitystandards adopted under this Article.*	Based on a review of all available information, including standards, trust levels and incidents, the State CIO recommends improvements to agency information security programs. The State CIO may assume direct responsibility for information technology security where agencies fail to adhere to adopted security standards. The exercise of the State CIO's discretion in assuming direct responsibility for providing an agency's information security program requires a carefully proscribed procedure and an accompanying funding mechanism. Actions are based on risk assessments and resource availability.
147-33.111	*All information technology security purchased using State funds, or for use by a state agency or in a State facility, shall be subject to approval by the State Chief*	The State CIO sets processes and procedures for approval of information technology security purchased with state

Section	Statement	Compliance Procedures
	Information Officer in accordance with security standards adopted under this Article.	funds.
147-33.111	*The State CIO shall conduct assessments of network vulnerability, including network penetration or any similar procedure. The State CIO may contract with another party or parties to perform the assessments. Detailed reports of the security issues identified shall be kept confidential as provided in G.S. 132-6.1(c)*	State CIO sets processes and procedures to perform security assessments. ESRMO coordinates security assessments for the State CIO and advises State CIO on assessment results.
147-33.111	*The legislative branch, judicial branch, the University of North Carolina and its constituent institutions, local school administrative units and the community college system may develop their own security standards that are comparable to or exceed those set by the State CIO. If they do, approval by the State CIO is not required before the purchase of information technology security.*	Where there are no comparable security standards for the entity, the State CIO's security standards, processes and procedures for approval of security technology purchases apply. Entities must notify the State CIO and obtain advance approval that the purchase meets State security standards.
147-33.111	*The State CIO shall consult with the legislative branch, judicial branch, the University of North Carolina and its constituent institutions, local school administrative units and the community college system in reviewing the security standards adopted by those entities.*	State CIO sets processes and procedures to consult and review security standards. ESRMO provides consultative services and reviews security standards for the State CIO.
147-33.111	*Before a State agency may enter into any contract with another party for an assessment of network vulnerability, the State agency must notify the State CIO and receive approval of the request. If the State agency enters into a contract for assessment and testing, after approval by the State CIO, the agency must provide the State CIO with copies of the detailed reports. The reports may not be disclosed as provided in G.S. 132-6.1(c).*	State CIO sets procedures to review and approve assessments of network security vulnerability. ESRMO coordinates these requests for the State CIO. Agencies or other parties must adhere to the review and approval process, including notification to ESRMO of plans prior to procuring assessments.
147-33.112	*The State Chief Information Officer shall assess the ability of each agency to comply with the current security enterprise-wide set of standards established pursuant to this section. The assessment shall include, at a minimum, the rate of compliance with the standards in each agency and an assessment of each agency's security organization, network security architecture, and current expenditures for information technology security. The assessment shall also estimate the cost to implement the security measures needed for agencies to fully comply with the standards. Each agency subject to the standards shall submit information required by the State Chief Information Officer for purposes of this assessment. The State Chief Information Officer shall include the information obtained from the assessment in the State Information Technology Plan required under G.S. 14733.72B.*	The State CIO: • Provides assessment tool(s) • Coordinates the assessments • Prepares metrics and reports • Includes the information in the Biennial State Information Technology Plan
147-33.113	*(a) The head of each State agency shall cooperate with the State Chief Information Officer in the discharge of his*	Agencies: • Report information technology

Section	Statement	Compliance Procedures
	or her duties by: *(1) Providing the full details of the agency's information technology and operational requirements and of all the agency's information technology security incidents within 24 hours of confirmation.* *(2) Providing comprehensive information concerning the information technology security employed to protect the agency's information technology.* *(3) Forecasting the parameters of the agency's projected future information technology security needs and capabilities.* *(4) Designating an agency liaison in the information technology area to coordinate with the State Chief Information Officer. The liaison shall be subject to a criminal background report from the State Repository of Criminal Histories, which shall be provided by the State Bureau of Investigation upon its receiving fingerprints from the liaison.* *If the liaison has been a resident of this State for less than five years, the background report shall include a review of criminal information from both the State and National Repositories of Criminal Histories. The criminal background report shall be provided to the State Chief Information Officer and the head of the agency. In addition, all personnel in the Office of State Auditor who are responsible for information technology security reviews pursuant to G.S. 147-64.6(c)(18) shall be subject to a criminal background report from the State Repository of Criminal Histories, which shall be provided by the State Bureau of Investigation upon receiving fingerprints from the personnel designated by the State Auditor. For designated personnel who have been residents of this State for less than five years, the background report shall include a review of criminal information from both the State and National Repositories of Criminal Histories. The criminal background reports shall be provided to the State Auditor.* *(b) The information provided by State agencies to the State Chief Information Officer under this section is protected from public disclosure pursuant to G.S. 132-6.1(c).*	security incidents to the ESRMO within 24 hours • Upon request, submit information technology security information to the State CIO for review • Designate agency security liaisons to coordinate with the State CIO • Obtain background checks for agency security liaisons and submit the results to the State CIO • Develop internal processes to comply with statewide security standards and practices and to fulfill all obligations concerning agency reporting to the State CIO • Develop internal processes, such as non-disclosure agreements to manage their distribution of confidential security information • Provide cost projections of future information technology security needs as part of the expansion budget preparation process The ESRMO maintains a database of security liaison information and generates reports as needed. The State CIO, as part of the assessment process, may request that each agency provide evidence of compliance on an annual basis and report the status of agencies' compliance to the Information Technology Advisory Board (ITAB). Requests to ITS for security information concerning an agency are referred to the agency security liaison for proper disposition. Staff in the Office of State Auditor (OSA) responsible for information security reviews must have criminal background checks performed by the SBI. The results of these checks are reported to the State Auditor.
G.S. 147-33.89	*Business continuity planning.* *(a) Each State agency shall develop and continually review and update as necessary a business and disaster recovery plan with respect to information technology. Each agency shall establish a disaster recovery planning team to develop the disaster recovery plan and to administer implementation of the plan. In developing the plan, the disaster recovery planning team shall do all of*	State agencies develop and update information technology business continuity plans using enterprise tools and methodologies. Agencies submit a business and disaster recovery plan to the State CIO annually and comply with state policies, standards,

Section	Statement	Compliance Procedures
	the following: *(1) Consider the organizational, managerial, and technical environments in which the disaster recovery plan must be implemented.* *(2) Assess the types and likely parameters of disasters most likely to occur and the resultant impacts on the agency's ability to perform its mission.* *(3) List protective measures to be implemented in anticipation of a natural or man-made disaster.* *(b) Each State agency shall submit its disaster recovery plan on an annual basis to the State Chief Information Officer.*	and procedures for business continuity planning. The State CIO, through the ESRMO, reviews the plans and reports the review results to the individual agencies. The ESRMO maintains the statewide cyber security incident response plan that supports recovery efforts in the event of an interruption of IT services due to an a cyber attack. Agencies develop cyber incident plans for their critical business systems using the statewide standards, templates and guidelines.
147-33.72B	*Planning and financing State information technology resources.* *(a) In order to provide a systematic process for meeting the State's technology needs, the State Chief Information Officer shall develop a biennial State Information Technology Plan (Plan). The Plan shall be transmitted to the General Assembly by February 1 of each regular session.* *(b) The Plan shall include the following elements:* *(1) An inventory of current information technology assets and major projects currently in progress. As used in this subdivision, the term 'major project' includes projects subject to review and approval under G.S. 147-33.72C, or that cost more than five hundred thousand dollars ($500, 000) to implement.* *(2) An evaluation and estimation of the significant unmet needs for information technology resources over a five -year time period. The Plan shall rank the unmet needs in priority order according to their urgency.* *(3) A statement of the financial requirements posed by the significant unmet needs together with a recommended funding schedule for each major project currently in progress or recommended for initiation during the upcoming fiscal biennium.* *(4) An analysis of opportunities for statewide initiatives that would yield significant efficiencies or improve effectiveness in State programs.* *(c) Each executive agency shall biennially develop an agency information technology plan that includes the information required under subsection (b) of this section. The Office of Information Technology Services shall consult with and assist agencies in the preparation of these plans. Each agency shall submit its plan to the State Chief Information Officer by October 1 of each even numbered year.*	ESRMO collects security, risk and business continuity management metrics and prepares reports for the State CIO. Appropriate information about security assets, major security projects and unmet security, risk management and business continuity needs are included in the State CIO's State Information Technology Plan. ESRMO prepares a strategic plan for security and risk management to support the State CIO's IT plan. Agencies are expected to include similar information in their IT plans.

Section	Statement	Compliance Procedures
147-33.72C	*Project approval standards.* *(a) Project Review and Approval – The State Chief Information Officer shall:* *(1) Review all State agency information technology projects that cost or are expected to cost more than five hundred thousand dollars ($500,000), whether the project is undertaken in a single phase or component or in multiple phases or components. If the State Chief Information Officer determines a project meets the quality assurance requirements established under this Article, the State Chief Information Officer shall approve the project.* *(2) Establish thresholds for determining which information technology projects costing or expected to cost five hundred thousand dollars ($500, 000) or less shall be subject to review and approval under subdivision (a)(1) of this section. When establishing the thresholds, the State Chief Information Officer shall consider factors such as project cost, potential project risk, agency size, and projected budget.* *(b) Project Implementation – No State agency shall proceed with an information technology project that is subject to review and approval under subsection (a) of this section until the State CIO approves the project. If a project is not approved, the State CIO shall specify in writing to the agency the grounds for denying the approval. The State CIO shall provide this information to the agency within five business days of the denial.* *(c) Suspension of Approval – The State Chief Information Officer may suspend the approval of any information technology project that does not continue to meet the applicable quality assurance standards. This authority extends to any information technology project that costs more than five hundred thousand dollars ($500,000) to implement regardless of whether the project was originally subject to review and approval under subsection (a) of this section. If the State CIO suspends approval of a project, the State CIO shall specify in writing to the agency the grounds for suspending the approval. The State CIO shall provide this information to the agency within five business days of the suspension.* *The Office of Information Technology Services shall report any suspension immediately to the Office of the State Controller and the Office of State Budget and Management. The Office of State Budget and Management shall not allow any additional expenditure of funds for a project that is no longer approved by the State Chief Information Officer.* *(d) General Quality Assurance- Information technology projects that are not subject to review and approval under subsection (a) of this section shall meet all other standards established under this Article.* *(e) Performance Contracting. – All contracts between a State agency and a private party for information*	As part of the project management process the agency is asked to provide: • A security contact • A summary of the function of the application and the community of users • A classification of data for legal requirements, such as HIPAA, IRS rules, and state confidentiality statutes • A risk assessment • The security architecture As required, the State Chief Security and Risk Officer (State CSRO) reviews and advises on the adequacy of the planned information security and risk management measures and compliance with statewide security standards, policies and procedures. In cases where a proposed project security architecture is not in compliance with State security standards, the agency must apply for and receive security deviation request approval using the State CIO's deviation reporting process coordinated by the ESRMO. ESRMO tracks project related security deviation requests for the State CIO.

Section	Statement	Compliance Procedures
	technology projects shall include provisions for vendor performance review and accountability. The State CIO may require that these contract provisions include monetary penalties for projects that are not completed within the specified time period or that involve costs in excess of those specified in the contract. The State CIO may require contract provisions requiring a vendor to provide a performance bond.	
147-33.72E	*Project Management Standards* *(a) Agency Responsibilities. – Each agency shall provide for a project manager who meets the applicable quality assurance standards for each information technology project that is subject to approval under G.S. 143-33.72C(a). The project manager shall be subject to the review and approval of the State Chief Information Officer.* *The agency project manager shall provide periodic reports to the project management assistant assigned to the project by the State CIO under subsection (b) of this section. The reports shall include information regarding project costs, issues related to hardware, software, or training, projected and actual completion dates, and any other information related to the implementation of the information technology project.* *(b) State Chief Information Officer Responsibilities. – The State Chief Information Officer shall designate a project management assistant from the Office of Information Technology Services for projects that receive approval under G.S. 147-33.72C(a). The State Chief Information Officer may designate a project management assistant for any other information technology project.* *The project management assistant shall advise the agency with the initial planning of a project, the content and design of any request for proposals, contract development, procurement, and architectural and other technical reviews. The project management assistant shall also monitor agency progress in the development and implementation of the project and shall provide status reports to the State Chief Information Officer, including recommendations regarding continued approval of the project.*	ESRMO staff works with Enterprise Project Management Office (EPMO) assigned by the State CIO to address the security and risk management and business continuity issues as they arise.
120-230	*There is established the Joint Legislative Oversight Committee on Information Technology.... The Committee shall examine, on a continuing basis, system wide issues affecting State government information technology....*	The security policies and standards may be reported to the Joint Legislative Oversight Committee.

~End of Document~