**Advanced Transportation Management System**

**Software Integration Project**

12/16/2020

**Security Evaluation Form (SEf)**

Prepared for

**North Carolina Department of Information Technology - Transportation**



**Executive Summary**

The State of North Carolina Statewide Information Security Manual (SISM) was established by the State CIO under authority N.C.G.S § 143B-1375, 143B-1376, and 143B-1378 to identify and implement information technology security controls. The policies, guidelines and standards defined in the NC SISM applies to all systems and services that store, process, transmit, and/or could impact the security of State data.

**STATUTORY LAW**

<https://www.ncleg.gov/EnactedLegislation/Statutes/PDF/BySection/Chapter_143B/GS_143B-1375.pdf>

<https://www.ncleg.gov/EnactedLegislation/Statutes/PDF/BySection/Chapter_143B/GS_143B-1376.pdf>

<https://www.ncleg.gov/EnactedLegislation/Statutes/PDF/BySection/Chapter_143B/GS_143B-1378.pdf>

**POLICIES, GUIDELINES AND STANDARDS**

<https://it.nc.gov/resources/cybersecurity-and-risk-management/esrmo-initiatives/statewide-information-security/>

<https://it.nc.gov/documents/statewide-data-classification-and-handling-policy>

<https://archives.ncdcr.gov/documents/functional-schedule-state-agencies>

**Glossary of Information Technology Terms**

<https://it.nc.gov/documents/statewide-glossary-information-technology-terms>

<https://csrc.nist.gov/glossary>

**Purpose**

This report and its underlying assessment are intended to enable State Agencies to assess the Organization’s processes and security capabilities of systems used to host State Data.

**Outcomes**

Submission of this report by the Organization does not guarantee a state-ready designation, nor does it guarantee that the North Carolina Department of Transportation (NCDOT) will procure services from the Organization.

**Approach and Use of This Document**

This document identifies clear and objective security and compliance capability requirements, where possible, while also allowing for the presentation of more subjective information. The combination of objective requirements and subjective information enables NCDOT to render a readiness decision based on a more complete understanding of the Organization’s security posture and capabilities.

**Organization System Information**

|  |
| --- |
| Organization Name:  System Name:  Service Model: (e.g. IaaS, PaaS, SaaS)  FIPS PUB 199 System Security Level: (Moderate)  Fully Operational as of: Enter the date the system became fully operational.  Number of Customers (State/Others): Enter # of customers / # of other customers  Deployment Model: Is the service a Public Cloud, Government-Only Cloud, Federal Government-Only Cloud, or Other? If other, please describe.  System Functionality: Briefly describe the functionality of the system and service being provided. |

|  |  |
| --- | --- |
| **Information Security Questionnaire** | |
| 1. The [Statewide Information Security Manual (SISM)](https://it.nc.gov/resources/cybersecurity-and-risk-management/esrmo-initiatives/statewide-information-security) was established by the State CIO under authority N.C.G.S § 143B-1375, 143B-1376, and 143B-1378. The policies and standards defined in the SISM apply to all systems and services that store, process, transmit, and/or could impact the security of NCDOT Data. It is important to understand a SOC 2 Type II only indicates the Organization’s policies, standards, and procedures were assessed as being compliant with generic industry accepted practices. A SOC 2 Type II does not certify the Organization’s services as being compliant with the NCDOT’s information security policies, guidelines and standards (e.g., account lockout thresholds, employment background checks (local/State/Federal), minimum password requirements, data classification, change management, etc.). | |
| 1. The term **personally identifiable information** refers to information that can be used to distinguish or trace an individual’s identity, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as name, date and place of birth, employer, home and work addresses, email address, phone number, mother’s maiden name, etc.   The Organization’s proposed solution will process **High-Risk (Highly Restricted)** NCDOT data including that could be used to distinguish or trace an individual’s identity. | |
| 1. Describe the Organization’s methodology for acknowledging and maintaining compliance with NCDOT’s information security policies, guidelines and standards. 2. Is the Organization’s methodology documented in a policy or procedure document? 3. Does the Organization’s methodology extend to all third parties supporting your proposed solution? Please explain. | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Provide a copy of the Organization’s formal security crosswalk between the Organization’s policies/standards and the NCDOT’s information security policies, guidelines and standards? 2. Are there any security gaps between the Organization’s proposed solution and the NCDOT’s information security policies, guidelines and standards? If yes, explain each gap and provide details on how you will mitigate the risks. | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. The **System Security Plan (SSP)** provides a summary of the security requirements of the system and describes the controls for meeting those requirements and defines responsibilities and expected behavior of all individuals who access the system. The SSP also contains or references other key security-related documents for the information system such as a risk assessment, Corrective Actions Plan (CAP), accreditation documentation, privacy threshold and impact assessment, contingency plan, configuration management plan, security configuration checklists and system interconnection agreements as appropriate. 2. Provide a System Security Plan (SSP) that addresses all applicable aspects of the Organization’s proposed solution. Linked below is a copy of the State’s SSP template.   https://it.nc.gov/documents/system-security-plan-template | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. **Data Flow Diagrams**: The purpose of a data flow diagram is to graphically represent data in all forms as it traverses systems including what changes the data and where it is stored at any given time. Examples of what could be represented in this diagram include data elements (name, address, phone, etc), data format, encryption and compression, authentication, permissions, session and registration (HTTP, SNMP, FTP, IRC, SSH, SSL, TLS, DES, 3-DES, AES, SSH, IMAP, RPC, SQL, NFS, API’s, Sockets and WinSock).    1. Provide data flow diagram(s) of the Organization’s proposed solution. Attached is an example high-level data flow diagram. | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. **Network Architecture Diagrams**: The purpose of network architecture diagrams is to graphically represent the structure of a network and shows the components that make up a network and how they interact, including routers, devices, hubs, firewalls, servers, workstations, printer, etc. 2. Provide network architecture(s) of the Organization’s proposed solution. | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Does the Organization have a third-party risk assessment report that demonstrates the Organization’s compliance to industry accepted practices (e.g. **SOC 2 Type II**, ISO 27001, FedRAMP, etc) for the IT services they provide to the State?    1. Provide a copy of the Organization’s third-party risk assessment reports.    2. Describe in detail how the Organization will ensure all applicable third parties supporting the Organization’s proposed solution receive and maintain SOC 2 Type II or equivalent certifications for their roles in supporting the Organization’s proposed solution.    3. Does the Organization have formal agreements with third parties, such as for maintenance and service support for the Organization’s solution and service offering?   **NOTE**: *It is important to understand a SOC 2 Type II only indicates the Organization’s policies, standards, and procedures were assessed as being compliant with generic industry accepted practices. A SOC 2 Type II does not certify the Organization’s services as being compliant with the State’s information security policies, guidelines and standards (e.g., account lockout thresholds, employment background checks (local/State/Federal), minimum password requirements, data classification, change management, etc.). Organizations must periodically perform formal security crosswalks between the Organization’s policies/standards and the State’s policies/standards to ensure the proper security controls are in place to protect State data. (References: N.C.G.S § 143B-1375, § 143B-1378;* [*SISM PS-7*](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Personnel_Security.pdf)*,* [*CA-7*](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Security_Assessment_%26_Authorization.pdf)*,* [*RA-3*](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Risk_Assessment.pdf)*).* | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Describe in detail how the Organization’s proposed solution supports NCDOT’s **Multi‐factor authentication (MFA)** policy, guidelines and standards. Specifically speak to Remote Access ([SISM AC-17](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), and Nonlocal Maintenance ([SISM MA-4](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Maintenance.pdf)). 2. Does the Organization’s solution enforce MFA for all administrative functions? Explain in detail. 3. Does the Organization’s solution enforce MFA for all remote access to State data? Explain in detail. | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. The **North Carolina Identity Management Service (NCID)** is the standard identity and access management platform provided by the Department of Information Technology. NCID is a web-based application that provides a secure environment for state agency, local government, business and individual users to log in and gain access to real-time resources, such as customer-based applications and information retrieval.    1. Will the Organization’s proposed solution integrate with the State’s NCID solution?    2. Describe in detail how the Organization’s proposed solution will integrate with North Carolina Identity (NCID) Service.   **References:**  <https://it.nc.gov/ncid/>  <https://it.nc.gov/ncid-frequently-asked-questions>  <https://it.nc.gov/ncid-application-integration-requirements-airn-saml-based> | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Provide a list of all Organizations and third parties that support the Organization’s proposed solution along with a brief description of their roles and responsibilities. | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. All operating systems (OS) AND major application software components (e.g. Microsoft SQL, Apache Tomcat, Oracle Weblogic, etc.), must NOT be past N-1. Applications which are not operating on the most recent platform MUST have a roadmap to upgrade with a State approved timeline. 2. Does the Organization’s proposed solution support the State’s N-1 requirement? 3. Explain in detail how the Organization maintains the N-1 standard. | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Does the Organization’s proposed solution meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements? | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Does the Organization’s solution store, process and/or transmit State data outside the boundaries of the United States? If yes, explain in detail. | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Are FIPS 140-3 Validated or National Security Agency (NSA)-Approved cryptographic modules consistently used where cryptography is required? Explain in detail. | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Does the Organization’s solution encrypt State data in-transit and at rest? Explain in detail. | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Does the Organization’s solution use deprecated transport layer security protocols (e.g., SSL, TLS 1.0, TLS 1.1)? Explain in detail. | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. State requires minimum 8-character complex passwords (Upper, Lower, Special Character and Numerical)? 2. Explain in detail how the Organization’s proposed solution will enforce the State's password policies and standards (SISM [AC](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf), [IA](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Identification_and_Authentication.pdf), [MA](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Maintenance.pdf), [SC](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Communications_Protection.pdf), [SI](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Information_Integrity.pdf), [SA](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Service_Acquisition.pdf)). | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Explain in detail how the Organization’s solution detects, contains, and eradicates malicious software? [[SISM SI-3](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Information_Integrity.pdf), [SISM SI-3](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Information_Integrity.pdf), [SISM MA-3](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Maintenance.pdf)] | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Explain in detail how the Organization’s solution stores audit data in a tamper-resistant manner which meets chain of custody and any e-discovery requirements? [[SISM AU-7](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Audit_Accountability.pdf), [SISM AU-9](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Audit_Accountability.pdf)] | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Explain in detail how the Organization’s solution detects unauthorized or malicious use of the systems, including insider threat and external intrusions? [[SISM SI-4](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Information_Integrity.pdf), [SISM SI-4 (4)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Information_Integrity.pdf), [SISM SI-7](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Information_Integrity.pdf), [SISM SI-7 (7)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Information_Integrity.pdf)] | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Explain in detail how the Organization performs security code analysis and assess code for security flaws, as well as identify, track and remediate security flaws? [[SISM SA-11](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Service_Acquisition.pdf)] | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Explain in detail how the Organization’s records retention policies, standards, practices and technologies adhere to the State’s functional records schedule. [[DNCR Functional Schedule](https://files.nc.gov/dncr-archives/documents/files/functional_overview_rev2019_final.pdf), [DNCR Information Technology](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf), [DNCR Risk Management](https://files.nc.gov/dncr-archives/documents/files/16_riskmgmt_final_rev2018.pdf), [SISM AU-7](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Audit_Accountability.pdf), [SISM AU-11](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Audit_Accountability.pdf)]?   A “[Record](https://files.nc.gov/ncdit/documents/files/Statewide-Glossary-2020.pdf)” is defined as a set of data (logical and physical) treated as a unit. Examples include, but are not limited to, IT Security Program documents, data flow and architecture diagrams, system/application diagrams, change management activities, risk management activities, vulnerability scan results, system/application logs, etc.   1. [**911.3** Data Documentation Records](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf)   Records concerning data in automated systems; includes data element dictionary, file layout, code book or table, entity relationships tables, and other records related to the structure, management, and organization of data  RETAIN UNTIL: System is discontinued and/or replaced  PLUS: 3 years THEN: Destroy   1. [**914.<** Digitization and Scanning Records](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf)   Records concerning data entry and imaging operations; includes quality control records and paper records that are digitized.  RETAIN UNTIL: Digitized PLUS: 10 days THEN: Destroy NOTE: The digital surrogate becomes the record copy and must be retained according to the disposition instructions for that record type.   1. [**915.3** Electronic Records Policies](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf)   Records documenting the policies and procedures employed by the agency to maintain authentic and accessible electronic records.  RETAIN UNTIL: Superseded/Obsolete PLUS: 3 years  THEN: Destroy   1. [**924.1(1)** Network and System Security Records](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf)   Records documenting the security of networks and systems; includes records concerning firewalls, anti-virus programs, and other related records.  RETAIN FROM: Creation  PLUS: 1 year THEN: Destroy\*   1. [**924.1(2)** Network and System Security Records](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf)   records documenting access requests and authorizations, system access logs, and other related records  RETAIN FROM: Creation PLUS: 1 year THEN: Destroy   1. [**924.2** Network and System Security Records](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf)   Records documenting incidents involving unauthorized attempted entry or probes on data processing systems, information technology systems, telecommunications networks, and electronic security systems, including associated software and hardware; includes logs, extracts, compilations of data, and other related records  RETAIN FROM: Creation PLUS: 2 years THEN: Destroy\*   1. [**926.3** System Documentation](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf)   records documenting operating systems, application programs, structure and form of datasets, system structure, and system-to-system communication; includes system overviews, dataset inventories, server names, IP addresses, purpose of the systems, Organization-supplied documentation, installed software, and current source code.  RETAIN UNTIL: Superseded/Obsolete  PLUS: 3 years THEN: Destroy   1. [**1623.3** Disaster Recovery Records](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf)   Records concerning minor or routine agency recovery operations that are managed with minimal disruption to normal operations  RETAIN UNTIL: Complete PLUS: 3 years THEN: Destroy   1. [**1314.2** Consultant, Contractor, Provider, and Organization Due Diligence Records](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf)   Records documenting the evaluation of consultants, contractors, providers, and Organizations with whom the agency conducts business; includes financial stability, information security risk assessments, and other related records  RETAIN UNTIL: Contract expires PLUS: 2 years THEN: Destroy | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Does the Organization have the capability to notify the State within 24 hours of suspected and/or confirmed incidents? If not, explain in detail. | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. If the Organization’s proposed solution provides email “send as” capabilities, does it support DMARC and DKIM for email protection? If not, explain in detail. | *If the system does not support this feature, do not answer Y or N. Instead, state “Not Applicable” here.* |
| 1. Describe in detail how the Organization’s proposed solution supports NCDOT’s **Data Protection and Classification Policies**, guidelines, and standards. Specifically speak to Security Impact Analysis ([SISM CM-4](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Configuration_Management.pdf)), Media Protection Policy ([SISM MP-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Media_Protection.pdf)), Media Marking ([SISM MP-3](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Media_Protection.pdf)), Media Storage ([SISM MP-4](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Media_Protection.pdf)), Media Transport ([SISM MP-5](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Media_Protection.pdf)), Media Sanitization ([SISM MP-6](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Media_Protection.pdf)), Media Use ([SISM MP-7](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Media_Protection.pdf)), Prohibit Use Without Owner ([SISM MP-7(1)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Media_Protection.pdf)), Security Categorization ([SISM RA-2](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Risk_Assessment.pdf)), and the Statewide Data Classification Policy. | *Describe in detail how the Organization’s proposed solution supports NCDOT’s* ***Data Protection and Classification Policies****, guidelines, and standards.*  *Please address each of the SISM requirements listed in question #26 in your response. Please review and understand the SISM requirements before responding.* |
| 1. Describe in detail how the Organization’s proposed solution supports NCDOT’s **Incident Response** policy, guidelines and standards. Specifically speak to Incident Response Plan Testing ([SISM IR-3](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Incident_Response.pdf)), Incident Response Plan Testing ([SISM IR-3(2)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Incident_Response.pdf)), Incident Handling ([SISM IR-4](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Incident_Response.pdf)), Incident Monitoring ([SISM IR-5](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Incident_Response.pdf)), Incident Reporting ([SISM IR-6](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Incident_Response.pdf)), and Incident Response Plan ([SISM IR-8](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Incident_Response.pdf)). | *Describe in detail how the Organization’s proposed solution supports NCDOT’s Incident Response policy, guidelines and standards.*  *Please address each of the SISM requirements listed in question #27 in your response. Please review and understand the SISM requirements before responding.* |
| 1. Describe in detail how the Organization’s proposed solution supports NCDOT’s **Contingency Planning** policy, guidelines and standards. Specifically speak to Contingency Planning Policy ([SISM CP-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Contingency_Planning.pdf)), Contingency Plan ([SISM CP-2](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Contingency_Planning.pdf)), Contingency Plan Training ([SISM CP-3](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Contingency_Planning.pdf)), Contingency Plan Testing and Exercises ([SISM CP-4](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Contingency_Planning.pdf)), Contingency Plan Alternate Storage Site ([SISM CP-6](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Contingency_Planning.pdf)), Contingency Plan Alternate Processing Site ([SISM CP-7](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Contingency_Planning.pdf)), Information System Backup ([SISM CP-9](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Contingency_Planning.pdf)), Testing for Reliability/Integrity ([CP-9(1)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Contingency_Planning.pdf)), and Information System Recovery and Reconstitution ([SISM CP-10](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Contingency_Planning.pdf)). 2. Describe in detail how the Organization’s proposed solution recovers the system(s) to a known and functional state following an outage, breach, DoS attack, or disaster? [[SISM CP-2](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Contingency_Planning.pdf), [SISM CP-9](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Contingency_Planning.pdf), [SISM CP-10](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Contingency_Planning.pdf)] 3. Does the Organization’s solution have alternate storage and processing facilities? [[SISM CP-6](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Contingency_Planning.pdf), [SISM CP-7](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Contingency_Planning.pdf)]. If yes, explain in detail. 4. Does the Organization have service level agreements (SLAs) in place with all telecommunications providers? [[SISM CP-8](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Contingency_Planning.pdf)] 5. Provide a copy of the Organization’s Business Impact Analysis and Disaster Recovery Plan. Attached are example templates. | *Describe in detail how the Organization’s proposed solution supports NCDOT’s* ***Contingency Planning*** *policy, guidelines and standards.*  *Please address each of the SISM requirements listed in question #28 in your response. Please review and understand the SISM requirements before responding.* |
| 1. Describe in detail how the Organization’s proposed solution supports NCDOT’s **Configuration Management** policy, guidelines and standards. Specifically speak to Configuration Management Policy ([SISM CM-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Configuration_Management.pdf)), Baseline Configuration ([SISM CM-2](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Configuration_Management.pdf)), Configuration Change Control ([SISM CM-3](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Configuration_Management.pdf)), Security Impact Analysis ([SISM CM-4](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Configuration_Management.pdf)), Access Restrictions for Change ([SISM CM-5](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Configuration_Management.pdf)), Configuration Settings ([SISM CM-6](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Configuration_Management.pdf)), Least Functionality ([SISM CM-7](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Configuration_Management.pdf)), Information System Component Inventory ([SISM CM-8](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Configuration_Management.pdf)), Automated Unauthorized Component Detection ([SISM CM-8(3)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Configuration_Management.pdf)), Configuration Management Plan ([SISM CM-9](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Configuration_Management.pdf)), Software Usage Restrictions ([SISM CM-10](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Configuration_Management.pdf)), Separation of Duties ([SISM AC-5](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Remote Access ([SISM AC-17](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Timely Maintenance ([SISM MA-6](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Maintenance.pdf)), Continuous Monitoring ([SISM CA-7](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Security_Assessment_%26_Authorization.pdf)), Flaw Remediation ([SISM SI-2](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Information_Integrity.pdf)), Malicious Code Protection ([SISM SI-3](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Information_Integrity.pdf)), System Development Life Cycle ([SISM SA-3](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Service_Acquisition.pdf)), and Developer Configuration Management ([SISM SA-10](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Service_Acquisition.pdf)). 2. Provide a copy of the Organization’s Change Management Policy, Standards and Procedures. 3. Provide a copy of the Organization’s Configuration Management Plan, Policy, Standards and Procedures. 4. Does the Organization’s change management capability include a fully functioning Change Advisory Boards (CAB)/ Technical Review Boards (TRB)? 5. Does the Organization have and use development and/or test environments to verify changes before implementing them in the production environment? 6. Within the Organization’s proposed solution, are all products and services still actively supported by their respective Organizations? 7. Does the Organization have a lifecycle management plan that ensures products are updated before they reach the end of their Organization support period? 8. Below is an example Security Impact Analysis template ([SISM CM-4](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Configuration_Management.pdf)). | *Describe in detail how the Organization’s proposed solution supports NCDOT’s* ***Configuration Management*** *policy, guidelines and standards.*  *Please address each of the SISM requirements listed in question #29 in your response. Please review and understand the SISM requirements before responding.* |
| 1. Describe in detail how the Organization’s proposed solution supports NCDOT’s **System and Communications Protection** policy, guidelines and standards. Specifically speak to Policy ([SISM SC-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Communications_Protection.pdf)), Application Partitioning ([SISM SC-2](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Communications_Protection.pdf)), Information in Shared Resources ([SISM SC-4](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Communications_Protection.pdf)), Denial of Service Protection ([SISM SC-5](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Communications_Protection.pdf)), Boundary Protection ([SISM SC-7](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Communications_Protection.pdf)), Transmission Confidentiality and Integrity ([SISM SC-8](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Communications_Protection.pdf)), Network Disconnect ([SISM SC-10](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Communications_Protection.pdf)), Cryptographic Key Establishment and Management ([SISM SC-12](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Communications_Protection.pdf)), Cryptographic Protection ([SISM SC-13](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Communications_Protection.pdf)), Public Key Infrastructure Certificates ([SISM SC-17](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Communications_Protection.pdf)), and Mobile Code ([SISM SC-18](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Communications_Protection.pdf)). | *Describe in detail how the Organization’s proposed solution supports NCDOT’s* ***System and Communications Protection*** *policy, guidelines and standards.*  *Please address each of the SISM requirements listed in question #30 in your response. Please review and understand the SISM requirements before responding.* |
| 1. Describe in detail how the Organization’s proposed solution supports NCDOT’s **Identification & Authentication** policy, guidelines and standards. Specifically speak to Access Control ([SISM AC-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Account Management ([SISM AC-2](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Automated System Account Management ([SISM AC-2(1)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Removal of Temporary / Emergency Accounts ([SISM AC-2(2)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Disable Inactive Accounts ([SISM AC-2(3)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Automated Audit Actions ([SISM AC-2(4)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Access Enforcement ([SISM AC-3](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Information Flow Enforcement ([SISM AC-4](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Separation of Duties ([SISM AC-5](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Least Privilege ([SISM AC-6](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Unsuccessful Logon Attempts ([SISM AC-7](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), System Use Notification ([SISM AC-8](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Session Lock ([SISM AC-11](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Pattern-Hiding Displays ([SISM AC-11(1)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf), Session Termination ([SISM AC-12](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Remote Access ([SISM AC-17](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Remote Access Automated Monitoring / Control (SISM [AC-17(1)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Remote Access – Protection of Confidentiality / Integrity Using Encryption ([SISM AC-17(2)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Remote Access – Managed Access Control Points ([SISM AC-17(3)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Remote Access – Privileged Commands / Access ([SISM AC-17(4)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Access Control for Mobile Devices ([SISM AC-19](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Access Control for Mobile Devices – Full Device / Container- Based Encryption ([SISM AC-19(5)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Use of External Information Systems ([SISM AC-20](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Use of External Information Systems – Limits on Authorized Use ([SISM AC-20(1)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Information Sharing ([SISM AC-21](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), and Publicly Accessible Content ([SISM AC-22](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)). | *Describe in detail how the Organization’s proposed solution supports NCDOT’s* ***Identification & Authentication*** *policy, guidelines and standards.*  *Please address each of the SISM requirements listed in question #31 in your response. Please review and understand the SISM requirements before responding.* |
| 1. Describe in detail how the Organization’s proposed solution supports NCDOT’s **Media Protection** policy, guidelines and standards. Specifically speak to Policy ([SISM MP-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Media_Protection.pdf)), Media Access ([SISM MP-2](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Media_Protection.pdf)), Media Marking ([SISM MP-3](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Media_Protection.pdf)), Media Storage ([SISM MP-4](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Media_Protection.pdf)), Media Transport ([SISM MP-5](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Media_Protection.pdf)), Media Sanitization ([SISM MP-6](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Media_Protection.pdf)), Media Use ([SISM MP-7](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Media_Protection.pdf)), and Media Use – Prohibit Use Without Owner ([SISM MP-7(1)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Media_Protection.pdf)). | *Describe in detail how the Organization’s proposed solution supports NCDOT’s Media Protection policy, guidelines and standards*.  *Please address each of the SISM requirements listed in question #32 in your response. Please review and understand the SISM requirements before responding.* |
| 1. Describe in detail how the Organization’s proposed solution supports NCDOT’s **Personnel Security** policy, guidelines and standards. Specifically speak to Policy ([SISM PS-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Personnel_Security.pdf)), Position Risk Designation ([SISM PS-2](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Personnel_Security.pdf)), Personnel Screening ([SISM PS-3](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Personnel_Security.pdf)), Personnel Termination ([SISM PS-4](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Personnel_Security.pdf)), Personnel Transfer ([SISM PS-5](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Personnel_Security.pdf)), Access Agreements ([SISM PS-6](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Personnel_Security.pdf)), and Third-Party Personnel Security ([SISM PS-7](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Personnel_Security.pdf)). | *Describe in detail how the Organization’s proposed solution supports NCDOT’s* ***Personnel Security*** *policy, guidelines and standards.*  *Please address each of the SISM requirements listed in question #33 in your response. Please review and understand the SISM requirements before responding.* |
| 1. Describe in detail how the Organization’s proposed solution supports NCDOT’s **Risk Assessment** policy, guidelines and standards. Specifically speak to Policy ([SISM RA-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Risk_Assessment.pdf)), Security Categorization ([SISM RA-2](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Risk_Assessment.pdf)), Risk Assessment ([SISM RA-3](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Risk_Assessment.pdf)), Vulnerability Scanning ([SISM RA-5](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Risk_Assessment.pdf)), Vulnerability Scanning – Update Tool Capability ([SISM RA-5(1)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Risk_Assessment.pdf)), Vulnerability Scanning – Frequency of Updates ([SISM RA-5(2)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Risk_Assessment.pdf)), and Vulnerability Scanning – Privileged Access ([SISM RA-5(5)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Risk_Assessment.pdf)). | *Describe in detail how the Organization’s proposed solution supports NCDOT’s* ***Risk Assessment*** *policy, guidelines and standards.*  *Please address each of the SISM requirements listed in question #34 in your response. Please review and understand the SISM requirements before responding.* |
| 1. Describe in detail how the Organization’s proposed solution supports NCDOT’s **Physical & Environmental Protection** policy, guidelines and standards. Specifically speak to Policy ([SISM PE-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Physical_and_Environmental_Protection.pdf)), Physical Access Authorizations ([SISM PE-2](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Physical_and_Environmental_Protection.pdf)), Physical Access Control ([SISM PE-3](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Physical_and_Environmental_Protection.pdf)), Access Control for Transmission Medium ([SISM PE-4](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Physical_and_Environmental_Protection.pdf)), Access Control for Output Devices ([SISM PE-5](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Physical_and_Environmental_Protection.pdf)), Monitoring Physical Access ([SISM PE-6](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Physical_and_Environmental_Protection.pdf)), Monitoring Physical Access – Intrusion Alarms ([SISM PE-6(1)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Physical_and_Environmental_Protection.pdf)), Visitor Access Records ([SISM PE-8](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Physical_and_Environmental_Protection.pdf)), Power Equipment and Cabling ([SISM PE-9](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Physical_and_Environmental_Protection.pdf)), Emergency Power ([SISM PE-11](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Physical_and_Environmental_Protection.pdf)), Fire Protection ([SISM PE-13](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Physical_and_Environmental_Protection.pdf)), Fire Protection – Automatic Fire Suppression ([SISM PE-13(3)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Physical_and_Environmental_Protection.pdf)), Delivery and Removal ([SISM PE-16](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Physical_and_Environmental_Protection.pdf)), Alternate Work Site ([SISM PE-17](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Physical_and_Environmental_Protection.pdf)), and Location of Information System Components ([SISM PE-18](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Physical_and_Environmental_Protection.pdf)). | *Describe in detail how the Organization’s proposed solution supports NCDOT’s* ***Physical & Environmental Protection*** *policy, guidelines and standards.*  *Please address each of the SISM requirements listed in question #35 in your response. Please review and understand the SISM requirements before responding.* |
| 1. When Critical or High software vulnerability are identified and patching is not an option, what Continuous Monitoring activities does the Organization perform to maintain visibility and identify if the known vulnerabilities been exploited? 2. How does the Organization track known vulnerabilities that can’t be patched or remediated? 3. Explain how the Organization maintains their [Corrective Actions Plan (CAP)](https://it.nc.gov/document/corrective-action-plan-cap-and-instructions), including timely, accurate, and complete information entries for new scan findings, Organization check-ins, and closure of CAP items? | *Organization provides comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. **Policies, Procedures, and Training**   The Organization must indicate the current status of their policy and procedure coverage.  To answer “**Yes**” to a policy, it must be fully developed, documented, and disseminated; and it must address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. A single policy document may address more than one family provided the requirements of each “-1” are fully addressed.  Organizations must establish their own set of Policies and Procedures (P&Ps). They cannot be inherited from a leveraged system, nor can they be provided by the customer or other third parties. Any exceptions and/or missing policy and procedure elements must be explained in comments section. | |

| **Family** | **Policy** | | **Standards** | | **Procedures** | | **Document Title, Version, and Last Review Date** | **Comments** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Yes** | **No** | **Yes** | **No** | **YES** | **No** |
| Access Control  [[SISM AC-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Awareness & Training  [[SISM AT-1](https://it.nc.gov/resources/cybersecurity-risk-management/esrmo-initiatives/statewide-information-security-policies#personnel-security)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Audit & Accountability [[SISM AU-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Audit_Accountability.pdf)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Security Assessment & Authorization  [[SISM CA-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Security_Assessment_%26_Authorization.pdf)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Configuration Management  [[SISM CM-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Configuration_Management.pdf)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Contingency Planning  [[SISM CP-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Contingency_Planning.pdf)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Identification & Authentication  [[SISM IA-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Identification_and_Authentication.pdf)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Incident Response  [[SISM IR-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Incident_Response.pdf)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Maintenance  [[SISM MA-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Maintenance.pdf)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Media Protection  [[SISM MP-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Media_Protection.pdf)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Physical & Environmental Protection  [[SISM PE-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Physical_and_Environmental_Protection.pdf)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Personnel Security  [[SISM PS-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Personnel_Security.pdf)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Risk Assessment  [[SISM RA-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Risk_Assessment.pdf)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| System & Services Acquisition  [[SISM SA-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Service_Acquisition.pdf)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| System & Communications Protection  [[SISM SC-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Communications_Protection.pdf)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| System & Information Integrity  [[SISM SI-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Information_Integrity.pdf)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Planning  [[SISM PL-1]](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Security_Planning.pdf) |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |

|  |  |
| --- | --- |
| **Organization Name:** |  |
| **Authorized Signature:** |  |
| **Name and Titled (Typed):** |  |
| **Date:** |  |