**COVER PAGE**

**Sample System Security Plan Template**

**Provided during the information security training workshop**

**Hosted by the North Carolina Department of Information Technology**

**Presented by JANUS Associates**

**January 30 and 31, 2018**

The purpose of this template is to provide a starting point for participants to document the security controls in their areas of responsibility. The System Security Plan (SSP) is a foundational document for organizations that adhere to the Risk Management Framework defined by the National Institute of Technology (NIST), as defined in the following NIST documents:

* SP 800-39 “Managing Information Security Risk: Organization, Mission, and Information System View”
* SP 800-37 Rev. 1: “Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach”
* SP 800-18 Rev. 1: “Guide for Developing Security Plans for Federal Information Systems”
* NIST SP 800-53 Rev. 4: “Recommended Security Controls for Federal Information Systems and Organizations”
* SP 800-30 Rev. 1: “Guide for Conducting Risk Assessments”

These and related documents are provided free of charge: <https://csrc.nist.gov/publications/sp800>

Although the NIST Risk Management Framework (RMF) was initially developed for use by the federal government, it has since been broadly adopted by many non-federal organizations in both the public and private sectors. The RMF was designed to be modified and adjusted to fit the specific context and requirements of each organization. JANUS Associates modified this template to align with the security control objectives and risk management program of the North Carolina Department of Information Technology. Participants are encouraged to further modify this template to align with their specific systems and information security requirements. Use of this template has not been mandated by official policy, as of the date of the training session.

*<<information system name>>* (*<<acronym>>*)

System Security Plan (SSP)

*<< month day, year >>*

Version Number: *<<vv.r>>*

REVIEW LOG

| **Date** | **Version** | **Description** | **Author** | **Approval** |
| --- | --- | --- | --- | --- |
| 9/21/2017 | 0.1 | Initial Draft | K.M., JANUS |  |
| 11/22/2017 | 0.2 | Updated Control Objectives | J.C., JANUS |  |
| 01/12/2018 | 1.0 draft | Updated to Template status | SJZ, JANUS |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Contents

[1. Statement of Purpose for the System Security Plan 11](#_Toc503491658)

[2. System Definition 11](#_Toc503491659)

[Information System Name/Title 11](#_Toc503491660)

[Information System Categorization: 11](#_Toc503491661)

[Information System Owner 11](#_Toc503491662)

[Authorizing Official 11](#_Toc503491663)

[Other Designated Contacts 11](#_Toc503491664)

[3. Concept of Operations 13](#_Toc503491665)

[3.1. Information System Description/Purpose 13](#_Toc503491666)

[3.2. System Environment 14](#_Toc503491667)

[3.3. System Interconnection/Information Sharing 15](#_Toc503491668)

[4. Security Controls 16](#_Toc503491669)

[4.1. Access Control (AC) 16](#_Toc503491670)

[AC-1 Access Control Policy and Procedures 16](#_Toc503491671)

[AC-2 Account Management 17](#_Toc503491672)

[AC-2(1) Automated System Account Management 18](#_Toc503491673)

[AC-2(2) Removal of Temporary / Emergency Accounts 19](#_Toc503491674)

[AC-2(3) Disable Inactive Accounts 20](#_Toc503491675)

[AC-2(4) Account Management | Automated Audit Actions 21](#_Toc503491676)

[AC-3 Access Enforcement 21](#_Toc503491677)

[AC-4 Information Flow Enforcement 22](#_Toc503491678)

[AC-5 Separation of Duties 22](#_Toc503491679)

[AC-6 Least Privilege 22](#_Toc503491680)

[AC-7 Unsuccessful Logon Attempts 24](#_Toc503491681)

[AC-8 System Use Notification 24](#_Toc503491682)

[AC-9 Previous Logon (Access) Notification 25](#_Toc503491683)

[AC-10 Concurrent Session Control 26](#_Toc503491684)

[AC-11 Session Lock 26](#_Toc503491685)

[AC-11(1) Session Lock | Pattern-hiding Displays 27](#_Toc503491686)

[AC-12 Session Termination 27](#_Toc503491687)

[AC-14 Permitted Actions without Identification or Authentication 28](#_Toc503491688)

[AC-16 Security Attributes 28](#_Toc503491689)

[AC-17 Remote Access 29](#_Toc503491690)

[AC-17(1) Remote Access | Automated Monitoring 29](#_Toc503491691)

[AC-17(2) Remote Access | Integrity Using Encryption 30](#_Toc503491692)

[AC-17(3) Remote Access | Managed Access Control Points 31](#_Toc503491693)

[AC-17(4) Remote Access | Privileged Commands 32](#_Toc503491694)

[AC-18 Wireless Access 32](#_Toc503491695)

[AC-18(1) Wireless Access | Authentication and Encryption 33](#_Toc503491696)

[AC-19 Access Control for Mobile Devices 33](#_Toc503491697)

[AC-19(5) Access Control for Mobile Devices | Encryption 34](#_Toc503491698)

[AC-20 Use of External Information Systems 34](#_Toc503491699)

[AC-20(1) Use of External Information Systems 35](#_Toc503491700)

[AC-20(2) Use of External Information Systems | Portable Storage Devices 36](#_Toc503491701)

[AC-21 Information Sharing 37](#_Toc503491702)

[AC-22 Publicly Accessible Content 38](#_Toc503491703)

[AC-23 Data Mining Protection 39](#_Toc503491704)

[AC-24 Access Control Decisions 39](#_Toc503491705)

[AC-25 Reference Monitor 40](#_Toc503491706)

[4.2. Awareness and Training (AT) 41](#_Toc503491707)

[AT-1 Security Awareness and Training Policy and Procedures 41](#_Toc503491708)

[AT-2 Security Awareness Training 41](#_Toc503491709)

[AT-2(2) Security Awareness | Insider Threat 42](#_Toc503491710)

[AT-3 Role-Based Security Training 42](#_Toc503491711)

[AT-4 Security Training Records 43](#_Toc503491712)

[4.3. Audit and Accountability (AU) 44](#_Toc503491713)

[AU-1 Audit and Accountability Policy and Procedures 44](#_Toc503491714)

[AU-2 Audit Events 44](#_Toc503491715)

[AU-2(3) Audit Events | Reviews and Updates 45](#_Toc503491716)

[AU-3 Content of Audit Records 45](#_Toc503491717)

[AU-3(1) Content of Audit Records | Additional Audit Information 46](#_Toc503491718)

[AU-4 Audit Storage Capacity 46](#_Toc503491719)

[AU-5 Response to Audit Processing Failures 47](#_Toc503491720)

[AU-6 Audit Review, Analysis, and Reporting 47](#_Toc503491721)

[AU-6(1) Audit Review, Analysis and Process | Process Integration 48](#_Toc503491722)

[AU-6(3) Audit Review, Analysis and Process | Correlate Audit Repositories 49](#_Toc503491723)

[AU-7 Audit Reduction and Report Generation 49](#_Toc503491724)

[AU-8 Time Stamps 50](#_Toc503491725)

[AU-8(1) Time Stamps | Synchronization With Authoritative Time Source 51](#_Toc503491726)

[AU-9 Protection of Audit Information 51](#_Toc503491727)

[AU-9(4) Protection of Audit Information | Access by Subset of Privileged Users 52](#_Toc503491728)

[AU-10 Non-repudiation 52](#_Toc503491729)

[AU-11 Audit Record Retention 52](#_Toc503491730)

[AU-12 Audit Generation 53](#_Toc503491731)

[AU-13 Monitoring for Information Disclosure 53](#_Toc503491732)

[AU-14 Session Audit 54](#_Toc503491733)

[AU-15 Alternate Audit Capability 55](#_Toc503491734)

[AU-16 Cross-Organizational Auditing 55](#_Toc503491735)

[4.4. Security Assessment and Authorization (CA) 56](#_Toc503491736)

[CA-1 Security Assessment and Authorization Policies and Procedures 56](#_Toc503491737)

[CA-2 Security Assessments 56](#_Toc503491738)

[CA-2(1) Security Assessments | Independent Assessors 57](#_Toc503491739)

[CA-3 System Interconnections 57](#_Toc503491740)

[CA-3(5) System Interconnections | Restrictions on External System Connections (Moderate Control) 59](#_Toc503491741)

[CA-5 Plan of Action and Milestones 59](#_Toc503491742)

[CA-6 Security Authorization 60](#_Toc503491743)

[CA-7 Continuous Monitoring 60](#_Toc503491744)

[CA-7(1) Continuous Monitoring | Independent Assessment 61](#_Toc503491745)

[CA-8 Penetration Testing 62](#_Toc503491746)

[CA-9 Internal System Connections 62](#_Toc503491747)

[4.5. Configuration Management (CM) 63](#_Toc503491748)

[CM-1 Configuration Management Policy and Procedures 63](#_Toc503491749)

[CM-2 Baseline Configuration 63](#_Toc503491750)

[CM-2(1) Baseline Configuration | Reviews and Updates 64](#_Toc503491751)

[CM-2(3) Baseline Configuration | Retention of Previous Configurations 65](#_Toc503491752)

[CM-2(7) Baseline Configuration | Configure Systems, Components, or Devices for High Risk Areas 66](#_Toc503491753)

[CM-3 Configuration Change Control 66](#_Toc503491754)

[CM-4 Security Impact Analysis 68](#_Toc503491755)

[CM-5 Access Restrictions for Change 68](#_Toc503491756)

[CM-6 Configuration Settings 68](#_Toc503491757)

[CM-7 Least Functionality 69](#_Toc503491758)

[CM-8 Information System Component Inventory 70](#_Toc503491759)

[CM-8(3) Information System Component Inventory | Updates During Installation 71](#_Toc503491760)

[CM-9 Configuration Management Plan 72](#_Toc503491761)

[CM-10 Software Usage Restrictions 72](#_Toc503491762)

[CM-11 User-Installed Software 73](#_Toc503491763)

[4.6. Contingency Planning (CP) 74](#_Toc503491764)

[CP-1 Contingency Planning Policy and Procedures 74](#_Toc503491765)

[CP-2 Contingency Plan 74](#_Toc503491766)

[CP-3 Contingency Plan Training 76](#_Toc503491767)

[CP-4 Contingency Plan Testing and Exercises 76](#_Toc503491768)

[CP-4(1) Contingency Plan Testing and Exercises | Coordinate with Other Related Plans 77](#_Toc503491769)

[CP-6 Contingency Plan Alternate Storage Site 77](#_Toc503491770)

[CP-6(1) Contingency Plan Alternate Storage Site | Separation from Primary Site 78](#_Toc503491771)

[CP-6(3) Contingency Plan Alternate Storage Site | Accessibility 79](#_Toc503491772)

[CP-7 Contingency Plan Alternate Processing Site 80](#_Toc503491773)

[CP-7(1) Contingency Plan Alternate Processing Site | Separation from Primary Site 81](#_Toc503491774)

[CP-7(2) Contingency Plan Alternate Processing Site | Accessibility 82](#_Toc503491775)

[CP-7(3) Contingency Plan Alternate Processing Site | Priority of Service 83](#_Toc503491776)

[CP-8 Telecommunications Services 84](#_Toc503491777)

[CP-9 Information System Backup 85](#_Toc503491778)

[CP-9(1) Information System Backup | Testing for Reliability / Integrity 85](#_Toc503491779)

[CP-10 Information System Recovery and Reconstitution 86](#_Toc503491780)

[CP-11 Alternate Communications Protocols 86](#_Toc503491781)

[CP-12 Safe Mode 87](#_Toc503491782)

[CP-13 Alternative Security Mechanisms 88](#_Toc503491783)

[4.7. Identification and Authorization (IA) 89](#_Toc503491784)

[IA-1 Identification and Authentication Policy and Procedures 89](#_Toc503491785)

[IA-2 Identification and Authentication Authorized Users 89](#_Toc503491786)

[IA-3 Device Identification and Authentication 90](#_Toc503491787)

[IA-4 Identifier Management 90](#_Toc503491788)

[IA-5 Authenticator Management 91](#_Toc503491789)

[IA-6 Authenticator Feedback 93](#_Toc503491790)

[IA-7 Cryptographic Module Authentication 93](#_Toc503491791)

[IA-8 Identification and Authentication (Non-Agency Users) 93](#_Toc503491792)

[IA-9 Service Identification and Authentication 94](#_Toc503491793)

[IA-10 Adaptive Identification and Authentication 94](#_Toc503491794)

[IA-11 Re-authentication 95](#_Toc503491795)

[4.8. Incident Response (IR) 96](#_Toc503491796)

[IR-1 Incident Response Policy and Procedures 96](#_Toc503491797)

[IR-2 Incident Response Plan Training 96](#_Toc503491798)

[IR-3 Incident Response Plan Testing 97](#_Toc503491799)

[IR-3(2) Incident Response Plan Testing | Coordination With Related Plans 98](#_Toc503491800)

[IR-4 Incident Handling 98](#_Toc503491801)

[IR-5 Incident Monitoring 100](#_Toc503491802)

[IR-6 Incident Reporting 101](#_Toc503491803)

[IR-7 Incident Response Assistance 102](#_Toc503491804)

[IR-8 Incident Response Plan 102](#_Toc503491805)

[IR-9 Information Spillage Response 103](#_Toc503491806)

[IR-10 Integrated Information Security Analysis Team 104](#_Toc503491807)

[4.9. Maintenance (MA) 105](#_Toc503491808)

[MA-1 System Maintenance Policy and Procedures 105](#_Toc503491809)

[MA-2 Controlled Maintenance 105](#_Toc503491810)

[MA-3 Maintenance Tools 106](#_Toc503491811)

[MA-3(1) Maintenance Tools | Inspect Tools 107](#_Toc503491812)

[MA-3(2) Maintenance Tools | Inspect Media 108](#_Toc503491813)

[MA-4 Nonlocal Maintenance 108](#_Toc503491814)

[MA-4(2) Nonlocal Maintenance | Document Nonlocal Maintenance 109](#_Toc503491815)

[MA-5 Maintenance Personnel 109](#_Toc503491816)

[MA-6 Timely Maintenance 110](#_Toc503491817)

[4.10. Media Protection (MP) 111](#_Toc503491818)

[MP-1 Media Protection Policy and Procedures 111](#_Toc503491819)

[MP-2 Media Access 111](#_Toc503491820)

[MP-3 Media Marking 112](#_Toc503491821)

[MP-4 Media Storage 113](#_Toc503491822)

[MP-5 Media Transport 114](#_Toc503491823)

[MP-6 Media Sanitization 115](#_Toc503491824)

[MP-7 Media Use 115](#_Toc503491825)

[MP-7(1) Media Use | Prohibit Use Without Owner 116](#_Toc503491826)

[MP-8 Media Downgrading 117](#_Toc503491827)

[4.11. Physical and Environmental Protection (PE) 118](#_Toc503491828)

[PE-1 Physical and Environmental Protection Policy and Procedures 118](#_Toc503491829)

[PE-2 Physical Access Authorizations 118](#_Toc503491830)

[PE-3 Physical Access Control 118](#_Toc503491831)

[PE-4 Access Control for Transmission Medium 119](#_Toc503491832)

[PE-5 Access Control for Output Devices 120](#_Toc503491833)

[PE-6 Monitoring Physical Access 120](#_Toc503491834)

[PE-6(1) Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment 121](#_Toc503491835)

[PE-8 Visitor Access Records 121](#_Toc503491836)

[PE-9 Power Equipment and Cabling 122](#_Toc503491837)

[PE-10 Emergency Shutoff 123](#_Toc503491838)

[PE-11 Emergency Power 124](#_Toc503491839)

[PE-12 Emergency Lighting 124](#_Toc503491840)

[PE-13 Fire Protection 125](#_Toc503491841)

[PE-13(3) Fire Protection | Automatic Fire Suppression 125](#_Toc503491842)

[PE-14 Temperature and Humidity Controls 125](#_Toc503491843)

[PE-15 Water Damage Protection 126](#_Toc503491844)

[PE-16 Delivery and Removal 126](#_Toc503491845)

[PE-17 Alternate Work Site 127](#_Toc503491846)

[PE-18 Location of Information System Components 128](#_Toc503491847)

[PE-19 Information Leakage 128](#_Toc503491848)

[PE-20 Asset Monitoring and Tracking 129](#_Toc503491849)

[4.12. Planning (PL) 130](#_Toc503491850)

[PL-1 Security Planning Policy and Procedures 130](#_Toc503491851)

[PL-2 System Security Plan 131](#_Toc503491852)

[PL-2(3) System Security Plan | Plan / Coordinate with Other Organizational Entities 132](#_Toc503491853)

[PL-4 Rules of Behavior 132](#_Toc503491854)

[PL-4(1) Rules of Behavior | Social Media and Networking Restrictions 133](#_Toc503491855)

[PL-7 Security Concept of Operations 134](#_Toc503491856)

[PL-8 Information Security Architecture 134](#_Toc503491857)

[PL-9 Information Security Architecture 135](#_Toc503491858)

[4.13. Personnel Security (PS) 136](#_Toc503491859)

[PS-1 Personnel Security Policy and Procedures 136](#_Toc503491860)

[PS-2 Position Risk Designation 136](#_Toc503491861)

[PS-3 Personnel Screening 136](#_Toc503491862)

[PS-4 Personnel Termination 137](#_Toc503491863)

[PS-5 Personnel Transfer 137](#_Toc503491864)

[PS-6 Access Agreements 138](#_Toc503491865)

[PS-7 Third-Party Personnel Security 138](#_Toc503491866)

[PS-8 Personnel Sanctions 138](#_Toc503491867)

[4.14. Risk Assessment (RA) 140](#_Toc503491868)

[RA-1 Risk Assessment Policy and Procedures 140](#_Toc503491869)

[RA-2 Security Categorization 140](#_Toc503491870)

[RA-3 Risk Assessment 140](#_Toc503491871)

[RA-5 Vulnerability Scanning 141](#_Toc503491872)

[RA-5(1) Vulnerability Scanning | Update Tool Capability 142](#_Toc503491873)

[RA-5(2) Vulnerability Scanning | Update by Frequency 143](#_Toc503491874)

[RA-5(5) Vulnerability Scanning | Privileged Access 144](#_Toc503491875)

[RA-6 Technical Surveillance Countermeasures Survey 144](#_Toc503491876)

[4.15. System and Services Acquisition (SA) 145](#_Toc503491877)

[SA-1 SA Policy 145](#_Toc503491878)

[SA-2 Allocation of Resources 145](#_Toc503491879)

[SA-3 System Development Life Cycle 146](#_Toc503491880)

[SA-4 Acquisition Process 146](#_Toc503491881)

[SA-4(1) Acquisition Process – Functional Properties of Security Controls 147](#_Toc503491882)

[SA-4(2) Acquisition Process – Design/Implementation Information for Security Controls 148](#_Toc503491883)

[SA-4(9) Acquisition Process – Functions/Ports/Protocols/Services in Use 149](#_Toc503491884)

[SA-5 Information System Documentation 149](#_Toc503491885)

[SA-8 Security Engineering Principles 150](#_Toc503491886)

[SA-9 External Information System Services 151](#_Toc503491887)

[SA-9(2) External Information System Services – Identification of Functions / Ports / Protocols / Services 151](#_Toc503491888)

[SA-10 Developer Configuration Management 152](#_Toc503491889)

[SA-11 Developer Security Testing and Evaluation 153](#_Toc503491890)

[SA-12 Supply Chain Protection 154](#_Toc503491891)

[SA-13 Trustworthiness 155](#_Toc503491892)

[SA-14 Criticality Analysis 156](#_Toc503491893)

[SA-15 Development Process, Standards, and Tools 156](#_Toc503491894)

[SA-16 Developer Provided Training 157](#_Toc503491895)

[SA-17 Developer Security Architecture and Design 158](#_Toc503491896)

[SA-18 Tamper Resistance and Detection 159](#_Toc503491897)

[SA-19 Component Authenticity 159](#_Toc503491898)

[SA-20 Customized Development of Critical Components 160](#_Toc503491899)

[SA-21 Developer Screening 161](#_Toc503491900)

[SA-22 Unsupported System Component 162](#_Toc503491901)

[4.16. System and Communication Protection (SC) 163](#_Toc503491902)

[SC-1 System and Communications Protection Policy and Procedures 163](#_Toc503491903)

[SC-2 Application Partitioning 163](#_Toc503491904)

[SC-3 Security Function Isolation 164](#_Toc503491905)

[SC-4 Information in Shared Resources 164](#_Toc503491906)

[SC-5 Denial of Service Protection 165](#_Toc503491907)

[SC-6 Resource Availability 166](#_Toc503491908)

[SC-7 Boundary Protection 166](#_Toc503491909)

[SC-8 Transmission Confidentiality and Integrity 169](#_Toc503491910)

[SC-10 Network Disconnect 170](#_Toc503491911)

[SC-11 Trusted Path 171](#_Toc503491912)

[SC-12 Cryptographic Key Establishment and Management 171](#_Toc503491913)

[SC-13 Cryptographic Protection 171](#_Toc503491914)

[SC-15 Collaborative Computing Devices 172](#_Toc503491915)

[SC-16 Transmission of Security Attributes 172](#_Toc503491916)

[SC-17 Public Key Infrastructure Certificates 173](#_Toc503491917)

[SC-18 Mobile Code 173](#_Toc503491918)

[SC-19 Voice Over Internet Protocol 173](#_Toc503491919)

[SC-20 Secure Name /Address Resolution Service (Authoritative Source) 174](#_Toc503491920)

[SC-21 Secure Name /Address Resolution Service (Recursive or Caching Resolver) 174](#_Toc503491921)

[SC-22 Architecture and Provisioning for Name/Address Resolution Service 174](#_Toc503491922)

[SC-23 Session Authenticity 175](#_Toc503491923)

[SC-24 Fail in Known State 175](#_Toc503491924)

[SC-25 Thin Nodes 176](#_Toc503491925)

[SC-26 Honeypots 176](#_Toc503491926)

[SC-27 Platform-Independent Applications 177](#_Toc503491927)

[SC-28 Protection of Information at Rest 177](#_Toc503491928)

[SC-29 Heterogeneity 178](#_Toc503491929)

[SC-30 Concealment and Misdirection 178](#_Toc503491930)

[SC-31 Covert Channel Analysis 179](#_Toc503491931)

[SC-32 Information System Partitioning 180](#_Toc503491932)

[SC-34 Non-Modifiable Executable Programs 180](#_Toc503491933)

[SC-35 Honeyclients 181](#_Toc503491934)

[SC-36 Distributed Processing and Storage 182](#_Toc503491935)

[SC-37 Out-of-Band Channels 182](#_Toc503491936)

[SC-38 Operations Security 183](#_Toc503491937)

[SC-39 Process Isolation 184](#_Toc503491938)

[SC-40 Wireless Link Protection 184](#_Toc503491939)

[SC-41 Port and I/O Device Access 185](#_Toc503491940)

[SC-42 Sensor Capability and Data 185](#_Toc503491941)

[SC-43 Usage Restrictions 186](#_Toc503491942)

[SC-44 Detonation Chambers 187](#_Toc503491943)

[4.17. System and Information Integrity (SI) 188](#_Toc503491944)

[SI-1 System and Information Integrity Policy and Procedures 188](#_Toc503491945)

[SI-2 Flaw Remediation 188](#_Toc503491946)

[SI-2(2) Flaw Remediation | Automated Flaw Remediation Status 189](#_Toc503491947)

[SI-3 Malicious Code Protection 189](#_Toc503491948)

[SI-3(1) Malicious Code Protection | Central Management 190](#_Toc503491949)

[SI-3(2) Malicious Code Protection | Automatic Updates 191](#_Toc503491950)

[SI-4 Information System Monitoring 191](#_Toc503491951)

[SI-4(2) Information System Monitoring | Automated Tools for Real-Time Analysis 192](#_Toc503491952)

[SI-4(4) Information System Monitoring | Inbound And Outbound Communications Traffic 193](#_Toc503491953)

[SI-4(5) Information System Monitoring | System-Generated Alerts 194](#_Toc503491954)

[SI-5 Security Alerts, Advisories, and Directives 194](#_Toc503491955)

[SI-6 Security Function Verification 195](#_Toc503491956)

[SI-7 Software, Firmware, and Information Integrity 196](#_Toc503491957)

[SI-7(1) Software, Firmware, and Information Integrity | Integrity Checks 197](#_Toc503491958)

[SI-7(7) Software, Firmware, and Information Integrity | Integrity of Detection And Response 198](#_Toc503491959)

[SI-8 Spam Protection 199](#_Toc503491960)

[SI-8(1) Spam Protection | Central Management 200](#_Toc503491961)

[SI-8(2) Spam Protection | Automatic Updates 201](#_Toc503491962)

[SI-10 Information Input Validation 201](#_Toc503491963)

[SI-11 Error Handling 202](#_Toc503491964)

[SI-12 Information Handling and Retention 202](#_Toc503491965)

[SI-13 Predictable Failure Prevention 203](#_Toc503491966)

[SI-14 Non-Persistence 204](#_Toc503491967)

[SI-15 Information Output Filtering 204](#_Toc503491968)

[SI-16 Memory Protection 205](#_Toc503491969)

[SI-17 Fail-Safe Procedures 206](#_Toc503491970)

# Statement of Purpose for the System Security Plan

The *<<information system name>>* (*<<acronym>>*) System Security Plan (SSP) provides an overview of the *<<acronym>>* system components, operational boundaries, security requirements, and roles and responsibilities for managing the security of *<<acronym>>* services. SSP’s are fundamental to IT security risk management, as defined in the following supporting documents:

* Statewide Information Security Policies of North Carolina
* NIST Special Publication 800-53, Rev 4: “Security and Privacy Controls for Federal Information Systems and Organizations”
* NIST Special Publication 800-18, Rev 1: “Guide for Developing Security Plans for Federal Information Systems”
* NIST FIPS-199: ”Standards for Security Categorization of Federal Information and Information Systems”
* NIST Special Publication 800-30, Rev 1: “Guide for Conducting Risk Assessments”
* NIST Special Publication 800-37 Revision 1: “Guide for Applying Risk Management Framework to Federal Information Systems”

# System Definition

### Information System Name/Title

* *<<information system name>>* (*<<acronym>>*)

### Information System Categorization:

* FIPS 199 <<*MODERATE or LOW*>>

The *<<acronym>>* system and components have been designated as “<<*MODERATE or LOW*>>” impact, according to security classifications defined in NIST FIPS-199: “Standards for Security Categorization of Federal Information and Information Systems”. [[1]](#footnote-1)

### Information System Owner

* *<<name of system owner>>*, *<<system owner’s title>>*

### Authorizing Official

* *<<name of authorizing official>>*, *<<authorizing official’s title>>*

### Other Designated Contacts

* *<<name of 1st designated contact>>*, *<<contact’s title>>*
* *<<name of 2nd designated contact>>*, *<<contact’s title>>*
* *<<name of 3rd designated contact>>*, *<<contact’s title>>*

# Concept of Operations

This Section discusses the information system to provide a context for understanding how the security controls will protect agency data, information, services, and processes.

This section also provides context for understanding from where the information system inherits controls and where the information system potentially provides inheritable controls to other information systems.

Delete this box after completing this Section.

## Information System Description/Purpose

This Sub-Section provides a general description of the information system and the purpose of the information system, identifying the:

1. information system as a General Support System (GSS) or a Major Application (MA);
2. functions and services which the information system provides;
3. data/information which the information consumes, generates, &/or stores;
4. sub-systems composing the information system;
5. any minor application rolled into the information system’s authorization boundary and authority to operate authority;
6. the authorization boundary of the information system, i.e., the dividing line between the information system and the external systems which interact with &/or support the information system; and
7. user/customer base for the information system, e.g., agency personnel, personnel from other agencies, private businesses, state citizens, federal personnel.

Delete this box after completing this Sub-Section.

*<<Describe the information system purpose and use>>*

## System Environment

This Sub-Section describes technical aspects of the information system, including:

1. the facility or facilities where the information system and its components reside;
2. the security zones within the information system;
3. the technical factors raising special security concerns, e.g., personal digital assistants, tablet devices, smart phones, wireless technology; and
4. an overview of server hardware, network devices, operating system, application, middleware, DBMS, etc. technology in use within the information system.

Typically this Sub-Section includes relevant network diagrams.

Delete this box after completing this Sub-Section.

*<<Describe system environment of the information system>>*

## System Interconnection/Information Sharing

This Sub-Section lists the interconnections between the information system and external systems owned or operated by different organizations. For each connection provide:

* Name of system;
* Organization;
* Type of interconnection;
* Authorizations for interconnection (MOU/MOA, ISA);
* Date of agreement;
* FIPS 199 Category;
* Certification and accreditation status of system; and
* Name and title of authorizing official(s).

For systems with numerous interconnections, consider using a table format for listing the connections.

Delete this box after completing this Sub-Section.

*<<List system interconnections>>*

# Security Controls

This Section describes the implementation of security controls to protect the data and processes of the information system as required by the North Carolina Statewide Information Security Manual and the Statewide Information Security Policies.

In this Section, for each control:

1. Document how the security control is implemented or planned to be implemented and the status of the implementation effort.
2. Identify whether the control implementation is specific to the information system this SSP documents (system specific), partially inherited (hybrid control), or fully inherited (common control); for inherited aspects of the control, identify the organization or information system providing the inherited aspects of the control.
3. Document any scoping or limitation of the applicability of the control within or to the information system.
4. Identify and document any compensating control implemented in place of or in addition to the control to achieve the intent of the control.

## Access Control (AC)

### AC-1 Access Control Policy and Procedures

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops, documents, and disseminates to all covered personnel that utilize IT resources:
   1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
2. Reviews and updates the current:
   1. Access control policy reviewed annually, at a minimum.
   2. Access control procedures [Assignment: organization-defined frequency].

#### Control Implementation Description:

*<<Description of control implementation>>*

### AC-2 Account Management

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];
2. Assigns account managers for information system accounts;
3. Establishes conditions for group and role membership;
4. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
5. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
6. Creates, enables, modifies, disables, and removes information system accounts in accordance with documented agency account management procedures.
7. Monitors the use of information system accounts;
8. Notifies account managers:
   1. When accounts are no longer required;
   2. When users are terminated or transferred; and
   3. When individual information system usage or need-to-know changes;
9. Authorizes access to the information system based on:
   1. A valid access authorization;
   2. Intended system usage; and
   3. Other attributes as required by the agency or associated missions/business functions;
10. Reviews accounts for compliance with account management requirements at a minimum of annually for user accounts and semi-annually for privileged accounts/roles. and
11. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-2(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-2(1) Automated System Account Management

#### North Carolina / NIST 800-53 Control Objective:

The agency employs automated mechanisms to support the management of information system accounts.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-2(2) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-2(2) Removal of Temporary / Emergency Accounts

#### North Carolina / NIST 800-53 Control Objective:

The information system automatically disables or removes temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-2(3) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-2(3) Disable Inactive Accounts

#### North Carolina / NIST 800-53 Control Objective:

The information system automatically disables inactive accounts after ninety (90) days, except as specifically exempted by a security administrator.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-2(4) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-2(4) Account Management | Automated Audit Actions

#### North Carolina / NIST 800-53 Control Objective:

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies the appropriate agency-defined personnel of these events.

#### Control Implementation Description:

*<<Description of control implementation>>*

### AC-3 Access Enforcement

#### North Carolina / NIST 800-53 Control Objective:

The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

#### Control Implementation Description:

*<<Description of control implementation>>*

### AC-4 Information Flow Enforcement

#### North Carolina / NIST 800-53 Control Objective:

The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on the technical safeguards in place to protect the FTI and traffic flow policy requirements identified in control SC-7 (see SCIO-SEC-316-00).

#### Control Implementation Description:

*<<Description of control implementation>>*

### AC-5 Separation of Duties

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Separates:
   * System Administration, and System Auditing,
   * System Development and System Change Management,
   * System Operations and System Security Administration,
   * Security administration and Security Auditing (if possible), and
   * All financial applications where misuse could cause a direct financial loss;
2. Documents separation of duties of individuals; and
3. Defines information system access authorizations to support separation of duties.

#### Control Implementation Description:

*<<Description of control implementation>>*

### AC-6 Least Privilege

#### North Carolina / NIST 800-53 Control Objective:

Agencies shall employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with agency missions and business functions. Least privilege applies to the development, implementation, and production lifecycle of information systems. Agencies shall enforce the following.

1. Only authorized individuals shall perform updates to restricted or highly restricted data such as citizen and business databases, protected health information (PHI), or FTI.
2. The agency shall explicitly authorize access to security functions and security-relevant information. Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.

Explicitly authorized personnel include security administrators, system and network administrators, system maintenance personnel, system programmers, and other privileged users.

1. The agency shall restrict privileged accounts on the information system to a limited number of authorized individuals with a need to perform administrative duties. Privileged accounts, including super user accounts, are typically described as system administrator for various types of systems.
   1. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions.
   2. Agencies may differentiate in an application between allowed privileges for local accounts and for domain accounts provided the agency retains the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.
2. Information systems shall prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
   1. Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities.
   2. Non-privileged users are individuals that do not possess appropriate authorizations.
   3. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.
3. Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on agencies. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Information systems shall do the following:
   1. Audit the execution of privileged functions as described in the Audit and Accountability Policy, SCIO-SEC-303, Section AU-2, Audit Events.
   2. Prevent non-privileged users from executing privileged functions; including disabling, circumventing, or altering implemented security safeguards/countermeasures.
4. Administrators of multi-user systems, systems that allow for concurrent usage of the system by multiple persons, must have at least two user credentials. One of these user credentials must provide privileged access, with all activities logged; the other must be a normal user credential for performing the day-to-day work of an ordinary user.
5. Users of information system accounts, or roles, with access to sensitive information, shall use non-privileged accounts or roles when accessing non-privileged functions. This control enhancement limits exposure when operating from within privileged accounts or roles.

#### Control Implementation Description:

*<<Description of control implementation>>*

### AC-7 Unsuccessful Logon Attempts

#### North Carolina / NIST 800-53 Control Objective:

The information system:

1. Enforces a limit of three (3) consecutive invalid logon attempts by a user during a 120-minute period; and
2. Automatically locks the account/node for at least thirty (30) minutes when the maximum number of unsuccessful attempts is exceeded. This can be shortened if the end user successfully unlocks the account through a challenge question scenario or a system administrator, security administrator, or authorized service desk staff member re-enables the user’s account

#### Control Implementation Description:

*<<Description of control implementation>>*

### AC-8 System Use Notification

#### North Carolina / NIST 800-53 Control Objective:

The information system:

1. Displays to users a system use notification message (provided below) before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:
   1. Users are accessing a U.S. Government information system;
   2. Information system usage may be monitored, recorded, and subject to audit;
   3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
   4. Use of the information system indicates consent to monitoring and recording;
2. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and
3. For publicly accessible systems:
   1. Displays system use information [Assignment: organization-defined conditions], before granting further access;
   2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
   3. Includes a description of the authorized uses of the system.

*This is a government computer system and is the property of the State of North Carolina. This system may contain U.S. Government information, which is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of the data contained herein or in transit to/from this system may subject the individual to administrative disciplinary actions, criminal and civil penalties. Users have no expectation of privacy. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed, or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to Law Enforcement Personnel. ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING.*

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-9 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-9 Previous Logon (Access) Notification

#### North Carolina / NIST 800-53 Control Objective:

The information system notifies the user, upon successful logon (access) to the system, of the date and time of the last logon (access).

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-10 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-10 Concurrent Session Control

#### North Carolina / NIST 800-53 Control Objective:

The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].

#### Control Implementation Description:

*<<Description of control implementation>>*

### AC-11 Session Lock

#### North Carolina / NIST 800-53 Control Objective:

The information system:

1. Prevents further access to the system by initiating a session lock after fifteen (15) minutes of inactivity or upon receiving a request from a user; and
2. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-11(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-11(1) Session Lock | Pattern-hiding Displays

#### North Carolina / NIST 800-53 Control Objective:

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

#### Control Implementation Description:

*<<Description of control implementation>>*

### AC-12 Session Termination

#### North Carolina / NIST 800-53 Control Objective:

The information system automatically terminates a user session after thirty (30) minutes of inactivity. For some higher risk information systems, the requirement for a session idle timeout may be more stringent as determined by agency policy, industry standard (e.g., PCI DSS) or other regulations.

#### Control Implementation Description:

*<<Description of control implementation>>*

### AC-14 Permitted Actions without Identification or Authentication

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Identifies what user action can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and
2. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-16 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-16 Security Attributes

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment: organization-defined security attribute values] with information in storage, in process, and/or in transmission;
2. Ensures that the security attribute associations are made and retained with the information;
3. Establishes the permitted [Assignment: organization-defined security attributes] for [Assignment: organization-defined information systems]; and
4. Determines the permitted [Assignment: organization-defined values or ranges] for each of the established security attributes.

#### Control Implementation Description:

*<<Description of control implementation>>*

### AC-17 Remote Access

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
2. Authorizes remote access to the information system prior to allowing such connections.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-17(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-17(1) Remote Access | Automated Monitoring

#### North Carolina / NIST 800-53 Control Objective:

The information system monitors and controls remote access methods.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-17(2) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-17(2) Remote Access | Integrity Using Encryption

#### North Carolina / NIST 800-53 Control Objective:

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-17(3) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-17(3) Remote Access | Managed Access Control Points

#### North Carolina / NIST 800-53 Control Objective:

The information system routes all remote accesses through managed network access control points. Limiting the number of access control points for remote accesses reduces the attack surface for organizations.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-17(4) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-17(4) Remote Access | Privileged Commands

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for administrative functions; and
2. Documents the rationale for such access in the security plan for the information system.

#### Control Implementation Description:

*<<Description of control implementation>>*

### AC-18 Wireless Access

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
2. Authorizes wireless access to the information system prior to allowing such connections.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-18(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-18(1) Wireless Access | Authentication and Encryption

#### North Carolina / NIST 800-53 Control Objective:

The information system protects wireless access to the system using authentication of users and FIPS 140-2 compliant encryption.

#### Control Implementation Description:

*<<Description of control implementation>>*

### AC-19 Access Control for Mobile Devices

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
2. Authorizes the connection of mobile devices to organizational information systems.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-19(5) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-19(5) Access Control for Mobile Devices | Encryption

#### North Carolina / NIST 800-53 Control Objective:

The agency employs either full-device encryption or container encryption to protect the confidentiality and integrity of information on agency provided mobile devices.

#### Control Implementation Description:

*<<Description of control implementation>>*

### AC-20 Use of External Information Systems

#### North Carolina / NIST 800-53 Control Objective:

The agency establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

1. Access the information system from external information systems; and
2. Process, store, or transmit organization-controlled information using external information systems.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-20(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-20(1) Use of External Information Systems

#### North Carolina / NIST 800-53 Control Objective:

The agency permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the agency:

1. Verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan; or
2. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-20(2) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-20(2) Use of External Information Systems | Portable Storage Devices

#### North Carolina / NIST 800-53 Control Objective:

The agency restricts the use of organization-controlled portable storage devices by authorized individuals on external information systems.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-21 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-21 Information Sharing

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and
2. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-22 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-22 Publicly Accessible Content

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Designates individuals authorized to post information onto a publicly accessible information system;
2. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
3. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
4. Reviews the content on the publicly accessible information system for nonpublic information quarterly, at a minimum, and removes such information, if discovered.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-23 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-23 Data Mining Protection

#### North Carolina / NIST 800-53 Control Objective:

The agency employs [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to adequately detect and protect against data mining.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-24 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-24 Access Control Decisions

#### North Carolina / NIST 800-53 Control Objective:

The organization establishes procedures to ensure [Assignment: organization-defined access control decisions] are applied to each access request prior to access enforcement.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-25 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AC-25 Reference Monitor

#### North Carolina / NIST 800-53 Control Objective:

The information system implements a reference monitor for [Assignment: organization-defined access control policies] that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.

#### Control Implementation Description:

*<<Description of control implementation>>*

## Awareness and Training (AT)

### AT-1 Security Awareness and Training Policy and Procedures

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops, documents, and disseminates to all covered personnel that utilize IT resources.
   1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
2. Reviews and updates the current:
   1. Security awareness and training policy at least annually; and
   2. Security awareness and training procedures [Assignment: organization-defined frequency].

#### Control Implementation Description:

*<<Description of control implementation>>*

### AT-2 Security Awareness Training

#### North Carolina / NIST 800-53 Control Objective:

The agency provides basic security awareness training to information system users (including managers, senior executives, and contractors):

1. As part of initial training for new users;
2. When required by information system changes; and
3. Annually thereafter.

#### Control Implementation Description:

*<<Description of control implementation>>*

AT-2(2) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AT-2(2) Security Awareness | Insider Threat

#### North Carolina / NIST 800-53 Control Objective:

The agency includes security awareness training on recognizing and reporting potential indicators of insider threat.

#### Control Implementation Description:

*<<Description of control implementation>>*

### AT-3 Role-Based Security Training

#### North Carolina / NIST 800-53 Control Objective:

The agency provides role-based security training to personnel with assigned security roles and responsibilities:

1. Before authorizing access to the information system or performing assigned duties;
2. When required by information system changes; and
3. Annually thereafter.

#### Control Implementation Description:

*<<Description of control implementation>>*

### AT-4 Security Training Records

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
2. Retains individual training records for a period of five years.

#### Control Implementation Description:

*<<Description of control implementation>>*

## Audit and Accountability (AU)

### AU-1 Audit and Accountability Policy and Procedures

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops, documents, and disseminates to all covered personnel that utilize IT resources
   1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
2. Reviews and updates the current:
   1. Audit and accountability policy annually at a minimum; and
   2. Audit and accountability procedures [Assignment: organization-defined frequency].

#### Control Implementation Description:

*<<Description of control implementation>>*

### AU-2 Audit Events

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Determines that the information system is capable of auditing the following events:
   1. Detect unauthorized activity
   2. Specified audit events
   3. Abnormalities
2. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
3. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
4. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-2(3) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AU-2(3) Audit Events | Reviews and Updates

#### North Carolina / NIST 800-53 Control Objective:

The agency reviews and updates the audited events annually, or when a major change to the information system occurs.

#### Control Implementation Description:

*<<Description of control implementation>>*

### AU-3 Content of Audit Records

#### North Carolina / NIST 800-53 Control Objective:

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-3(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AU-3(1) Content of Audit Records | Additional Audit Information

#### North Carolina / NIST 800-53 Control Objective:

The information system generates audit records containing the following additional information:

* 1. Manufacturer-specific event name / type of event
  2. Full text recording of privileged commands
  3. Individual identities of group account users

#### Control Implementation Description:

*<<Description of control implementation>>*

### AU-4 Audit Storage Capacity

#### North Carolina / NIST 800-53 Control Objective:

The agency allocates audit record storage capacity to retain audit records for the required audit retention period of three years in accordance with the G116 Audit Trails File requirement stated in the NC [Department of Natural and Cultural Resources](http://www.ncdcr.gov/) State’s General Schedule for State Agency Records.

#### Control Implementation Description:

*<<Description of control implementation>>*

### AU-5 Response to Audit Processing Failures

#### North Carolina / NIST 800-53 Control Objective:

The information system:

1. Alerts must be sent to agency defined personnel or roles in the event of an audit processing failure; and
2. Takes the following additional actions:
   1. Provide a warning when allocated audit record storage volume reaches a maximum audit record storage capacity.
   2. The system should automatically alert designated officials in the event of an audit failure or when audit capacity is 70%, 80%, and again at 90% utilization. This alert should be sent by a mechanism that allows system administrators to receive it after hours (e.g., email, text message).
   3. Once the maximum storage capacity for audit logs is reached or there is an audit failure, the information system should overwrite the oldest audit records *or automatically shut down in an effort to eliminate the chance of an incident*, in the absence of auditing and accountability.

#### Control Implementation Description:

*<<Description of control implementation>>*

### AU-6 Audit Review, Analysis, and Reporting

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Reviews and analyzes information system audit records regularly for abnormalities and
2. Reports findings to agency management.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-6(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AU-6(1) Audit Review, Analysis and Process | Process Integration

#### North Carolina / NIST 800-53 Control Objective:

The agency employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

#### Control Implementation Description:

*<<Description of control implementation>>*

AC-6(3) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AU-6(3) Audit Review, Analysis and Process | Correlate Audit Repositories

#### North Carolina / NIST 800-53 Control Objective:

The agency analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

#### Control Implementation Description:

*<<Description of control implementation>>*

### AU-7 Audit Reduction and Report Generation

#### North Carolina / NIST 800-53 Control Objective:

1. Audit reduction and report generation capability shall be implemented that does the following:
   1. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents
   2. Does not alter the original content or time ordering of audit records.
2. The agency information system shall provide the capability to process audit records for events of interest based on AU-2. Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed.
3. Agencies may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component.
4. This control is optional for LOW risk information systems.

#### Control Implementation Description:

*<<Description of control implementation>>*

### AU-8 Time Stamps

#### North Carolina / NIST 800-53 Control Objective:

The information system:

1. Uses internal system clocks to generate time stamps for audit records; and
2. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets a DIT defined time synchronization and source.

#### Control Implementation Description:

*<<Description of control implementation>>*

AU-8(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AU-8(1) Time Stamps | Synchronization With Authoritative Time Source

#### North Carolina / NIST 800-53 Control Objective:

The information system:

1. Compares the internal information system clocks at an agency defined frequency to a DIT defined authoritative time source and
2. Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period].

#### Control Implementation Description:

*<<Description of control implementation>>*

### AU-9 Protection of Audit Information

#### North Carolina / NIST 800-53 Control Objective:

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

#### Control Implementation Description:

*<<Description of control implementation>>*

AU-9(4) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AU-9(4) Protection of Audit Information | Access by Subset of Privileged Users

#### North Carolina / NIST 800-53 Control Objective:

The agency authorizes access to management of audit functionality to agency-defined subset of privileged users].Control Implementation Description:

#### Control Implementation Description:

*<<Description of control implementation>>*

AU-10 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AU-10 Non-repudiation

#### North Carolina / NIST 800-53 Control Objective:

The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [Assignment: organization-defined actions to be covered by non-repudiation].

#### Control Implementation Description:

*<<Description of control implementation>>*

### AU-11 Audit Record Retention

#### North Carolina / NIST 800-53 Control Objective:

The agency retains audit records for at least three years per the G116 Audit Trails File requirement stated in the NC [Department of Natural and Cultural Resources](http://www.ncdcr.gov/) to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

#### Control Implementation Description:

*<<Description of control implementation>>*

### AU-12 Audit Generation

#### North Carolina / NIST 800-53 Control Objective:

The information system:

1. Provides audit record generation capability for the auditable events defined in AU-2.
2. Allows designated State and agency personnel to select which auditable events are to be audited by specific components of the information system; and
3. Generates audit records for the events defined in AU-2 d. with the content defined in AU-

#### Control Implementation Description:

*<<Description of control implementation>>*

AU-13 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AU-13 Monitoring for Information Disclosure

#### North Carolina / NIST 800-53 Control Objective:

The agency monitors [Assignment: organization-defined open source information and/or information sites] [Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information.

#### Control Implementation Description:

*<<Description of control implementation>>*

AU-14 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AU-14 Session Audit

#### North Carolina / NIST 800-53 Control Objective:

The information system provides the capability for authorized users to select a user session to capture/record or view/hear.

#### Control Implementation Description:

*<<Description of control implementation>>*

AU-15 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AU-15 Alternate Audit Capability

#### North Carolina / NIST 800-53 Control Objective:

The agency provides an alternate audit capability in the event of a failure in primary audit capability that provides [Assignment: organization-defined alternate audit functionality].

#### Control Implementation Description:

*<<Description of control implementation>>*

AU-16 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### AU-16 Cross-Organizational Auditing

#### North Carolina / NIST 800-53 Control Objective:

The agency employs [Assignment: organization-defined methods] for coordinating [Assignment: organization-defined audit information] among external organizations when audit information is transmitted across organizational boundaries.

#### Control Implementation Description:

*<<Description of control implementation>>*

## Security Assessment and Authorization (CA)

### CA-1 Security Assessment and Authorization Policies and Procedures

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops, documents, and disseminates to all personnel performing designated roles in the security assessment and authorization process:
   1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
2. Reviews and updates the current:
   1. Security assessment and authorization policy annually at a minimum.
   2. Security assessment and authorization procedures [Assignment: organization-defined frequency].

#### Control Implementation Description:

*<<Description of control implementation>>*

### CA-2 Security Assessments

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops a security assessment plan that describes the scope of the assessment including:
   1. Security controls and control enhancements under assessment;
   2. Assessment procedures to be used to determine security control effectiveness; and
   3. Assessment environment, assessment team, and assessment roles and responsibilities;
2. b. Assesses the security controls in the information system and its environment of operation will be assessed on an annual basis to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
3. Produces a security assessment report that documents the results of the assessment; and
4. Provides the results of the security control assessment to the State CIO.

#### Control Implementation Description:

*<<Description of control implementation>>*

CA-2(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CA-2(1) Security Assessments | Independent Assessors

#### North Carolina / NIST 800-53 Control Objective:

The agency employs third party assessors or assessment teams to conduct security control assessments.

#### Control Implementation Description:

*<<Description of control implementation>>*

### CA-3 System Interconnections

#### North Carolina / NIST 800-53 Control Objective:

All agency information systems must authorize connections from the information system to other information systems that do the following:

1. Connect through the use of Interconnection Security Agreements (ISAs), business associate agreement (BAA), service level agreement (SLA), etc.
2. For each connection, document the interface characteristics, security requirements, incident handling procedures, roles and responsibilities, costs incurred under the agreement and the nature of the information communicated.
3. Employ deny-all and allow-by-exception policy for allowing systems that receive, process, store, or transmit data to connect to external information systems.
4. Monitor the information assets connections on an annual basis verifying enforcement of security requirements.
5. Follow the procedures below for connections to systems outside of the State Network:
   1. An approved Memorandum of Understanding / Agreement (MOU/A) or Interconnection Security Agreement (ISA) signed by the State Chief Information Officer (SCIO) or designee or Agency CIO.
   2. Submit a connection request as well as a Privacy Threshold Analysis (PTA) document to the Department of Information Technology (DIT). The request shall include the following:
      1. Type of connection to be established
      2. Type Connection requirements
      3. Key personnel to help coordinate the planning efforts of the system interconnection
      4. Duration of the interconnection
      5. Point of contact for the external organization requesting the interconnection
      6. of data and level of sensitivity of the data being exchanged
   3. Prior to system interconnection, system owners must complete a security impact analysis. The results must be provided to the Agency CIO for risk determination and approval.
   4. Review and update ISAs at minimum annually or whenever there is a significant change to any of the interconnected systems.
   5. Terminate all interconnections when any of the following conditions are met:
      1. The ISA, MOU/MOA or SLA has expired or is withdrawn
      2. The business requirement for the interconnection no longer exists
      3. A significant change in the environment increases the risk to an unacceptable level of operations

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

#### Control Implementation Description:

*<<Description of control implementation>>*

CA-3(5) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CA-3(5) System Interconnections | Restrictions on External System Connections (Moderate Control)

#### North Carolina / NIST 800-53 Control Objective:

The organization employs either an allow-all, deny-by-exception; or deny-all, permit-by-exception policy for allowing restricted or highly restricted data to connect to external information systems.

#### Control Implementation Description:

*<<Description of control implementation>>*

### CA-5 Plan of Action and Milestones

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops a plan of action and milestones for the information system to document the agency’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
2. Updates existing plan of action and milestones quarterly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

#### Control Implementation Description:

*<<Description of control implementation>>*

### CA-6 Security Authorization

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Assigns a senior-level executive or manager as the authorizing official for the information system;
2. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
3. Updates the security authorization [Assignment: organization-defined frequency]

#### Control Implementation Description:

*<<Description of control implementation>>*

### CA-7 Continuous Monitoring

#### North Carolina / NIST 800-53 Control Objective:

The agency develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

1. Establishment of performance metrics to be monitored;
2. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring;
3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
4. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
5. Correlation and analysis of security-related information generated by assessments and monitoring;
6. Response actions to address results of the analysis of security-related information; and
7. Reporting the security status of organization and the information system to ESRMO within 30 days of completion of an assessment through the ESRMO EGRC repository

#### Control Implementation Description:

*<<Description of control implementation>>*

CA-7(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

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

#### North Carolina / NIST 800-53 Control Objective:

The agency employs assessors or assessment teams from third-party providers to monitor the security controls in the information system on an ongoing basis.

#### Control Implementation Description:

*<<Description of control implementation>>*

CA-8 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CA-8 Penetration Testing

#### North Carolina / NIST 800-53 Control Objective:

The agency conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components].

#### Control Implementation Description:

*<<Description of control implementation>>*

### CA-9 Internal System Connections

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Authorizes internal connections for agency defined classes and subclasses of components to the information system; and
2. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

#### Control Implementation Description:

*<<Description of control implementation>>*

## Configuration Management (CM)

### CM-1 Configuration Management Policy and Procedures

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops, documents, and disseminates to all covered personnel that utilize IT resources
   1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
2. Reviews and updates the current:
   1. Configuration management policy annually; and
   2. Configuration management procedures [Assignment: organization-defined frequency].

#### Control Implementation Description:

*<<Description of control implementation>>*

### CM-2 Baseline Configuration

#### North Carolina / NIST 800-53 Control Objective:

The agency develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

#### Control Implementation Description:

*<<Description of control implementation>>*

CM-2(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CM-2(1) Baseline Configuration | Reviews and Updates

#### North Carolina / NIST 800-53 Control Objective:

The agency reviews and updates the baseline configuration of the information system:

1. Annually at a minimum;
2. When required due to significant change in the baseline configuration, increase in interconnections with other systems outside the authorized boundary or significant changes in the security requirements of the system; and
3. As an integral part of information system component installations and upgrades.

#### Control Implementation Description:

*<<Description of control implementation>>*

CM-2(3) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CM-2(3) Baseline Configuration | Retention of Previous Configurations

#### North Carolina / NIST 800-53 Control Objective:

The agency retains previous versions of baseline configurations of the information system to support rollback.

#### Control Implementation Description:

*<<Description of control implementation>>*

CM-2(7) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CM-2(7) Baseline Configuration | Configure Systems, Components, or Devices for High Risk Areas

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Issues agency-defined information systems, system components, or devices with agency-defined configurations to individuals traveling to locations that the agency deems to be of significant risk; and
2. Applies safeguards to the devices when the individuals return, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive.

#### Control Implementation Description:

*<<Description of control implementation>>*

### CM-3 Configuration Change Control

#### North Carolina / NIST 800-53 Control Objective:

Agencies shall safeguard production systems during modification, including emergency changes. Agencies shall manage changes to systems and application programs to protect the systems and programs from failure as well as security breaches. Adequate management of system change control processes shall require the following:

1. Enforcement of formal change control procedures
2. Proper authorization and approvals at all levels
3. Successful testing of updates and new programs prior to their being moved into a production environment
4. Updates addressing significant security vulnerabilities shall be prioritized, evaluated, tested, documented, approved and applied promptly to minimize the exposure of unpatched resources. Vulnerability Management requirements are addressed in the System and Information Integrity Policy SCIO-SEC-317, Section SI-2.
5. Whenever an update is implemented, the application system the update affects shall be tested to ensure that business operations and security controls perform as expected.
6. Each agency shall enforce strict change control procedures because application software fundamentally affects the agency’s business and mission. Inadequate or poorly managed change control procedures can result in compromises and failures not only in the operational system being modified, but also in other systems that are dependent on the new functionality provided by the updated system.
7. When possible, agencies should integrate application change control and operational change control procedures. This effort should include the following processes, controls, and best practices:
   1. Controls and approval levels for updating libraries
   2. Requiring formal agreement and approval for any changes
   3. Restricting library content
   4. Restricting programmers’ access to only those parts of the system necessary for their work
   5. Version control for each application.
   6. Tying program documentation updates to source code updates
   7. Audit logs that track all accesses to libraries, copying and use of source code, and updates posted to libraries
8. Defining job responsibilities/restrictions and establishing authority levels for the following:
   1. Program librarian(s)
   2. Developers (i.e., should neither test their own code nor promote it into production)
   3. Other IT staff
9. Personnel authorized to make or submit changes to the source library (i.e., a program librarian) should be appointed for each major application to control check-in/check-out.
10. Training needs for business and technical users covering new features and security controls introduced by the upgrade
11. Rollback procedures designed to recover to previous stable version of programs

Agencies shall ensure that testing does not interfere with information system operations. Individuals/groups conducting tests understand State and agency security policies and procedures, information system security policies and procedures, and the specific health, safety, and environmental risks associated with particular facilities/processes. Operational systems may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If information systems must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. If testing cannot be conducted on operational systems, organizations employ compensating controls (e.g., testing on replicated systems).

#### Control Implementation Description:

*<<Description of control implementation>>*

### CM-4 Security Impact Analysis

#### North Carolina / NIST 800-53 Control Objective:

The agency analyzes changes to the information system to determine potential security impacts prior to change implementation.

#### Control Implementation Description:

*<<Description of control implementation>>*

### CM-5 Access Restrictions for Change

#### North Carolina / NIST 800-53 Control Objective:

The agency defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

#### Control Implementation Description:

*<<Description of control implementation>>*

### CM-6 Configuration Settings

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Establishes and documents configuration settings for information technology products employed within the information system using the following sources, listed in order of precedence that reflect the most restrictive mode consistent with operational requirements;
   1. NIST recommended configurations and checklists: <http://checklists.nist.gov/>
   2. Defense Information Systems Agency (DISA) security checklists and Standard Technical Implementation Guides (STIGs): <http://iase.disa.mil/stigs/stig/index.html>and <http://iase.disa.mil/stigs/checklist/index.html>
   3. National Security Agency (NSA) configuration guides: <http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml>
   4. Center for Internet Security (CIS) benchmarks: <https://benchmarks.cisecurity.org/downloads/benchmarks/>
   5. Safeguard Computer Security Evaluation Matrix (SCSEM): <https://www.irs.gov/uac/safeguards-program>, for systems that store, process, or transmit federal tax information (FTI).
2. Implements the configuration settings;
3. Identifies, documents, and approves any deviations from established configuration settings for information systems based on [Assignment: organization-defined operational requirements]; and
4. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

#### Control Implementation Description:

*<<Description of control implementation>>*

### CM-7 Least Functionality

#### North Carolina / NIST 800-53 Control Objective:

Agencies shall implement the following requirements to provide least functionality:

1. Configure information systems to provide only essential capabilities and specifically prohibit or restrict the use of functions, ports, protocols, and/or services that are not required for the business function of the information system.
2. Where feasible, the agency will limit component functionality to a single function per device (e.g., email server or web server, not both).
3. Employ an allow-all, deny by exception (blacklisting) policy to prohibit the execution of unauthorized software programs on State and agency information systems. Agencies can implement whitelisting, whereby a list of approved applications is given (deny-all, all-by-exception), if that is the preferred approach for restricting software program execution.
4. Disable any functions, ports, protocols, and services within an information system that are deemed to be unnecessary and/or non-secure. Agencies can either make a determination of the relative security of a function, port, protocol, and/or service or base a security decision on the assessment of other entities. The use of the following functions, ports, protocols, and/or services, at a minimum, must be specifically prohibited or restricted:
   1. Border Gateway Protocol (BGP) Port 179 / Transmission Control Protocol (TCP)
   2. Domain Name System be (DNS) Port 53 / TCP, User Datagram Protocol (UDP)
   3. File Transfer Protocol (FTP) Ports 20, 21 / TCP
   4. Finger Port 79 / TCP
   5. Hypertext Transfer Protocol (HTTP) Port 80 / TCP
   6. Internet Control Messaging Protocol (ICMP) - block incoming echo request (ping and Windows traceroute) block outgoing echo replies, time exceeded, and destination unreachable messages except "packet too big" messages (type 3, code 4). Note: Blocking ICMP will restrict legitimate use of PING in an effort to restrict malicious activity.
   7. Internet Message Access Protocol (IMAP) Port 143 / TCP, UDP
   8. Internet Relay Chat (IRC) Port 194 / UDP
   9. Lightweight Directory Access Protocol (LDAP) Port 389 / TCP, UDP
   10. Line Printer Daemon (LPD) Port 515 / TCP
   11. Network Basic Input Output System (NetBIOS) Port 137 / TCP, UDP
   12. Network News Transfer Protocol (NNTP) Port 119 / TCP
   13. Network Time Protocol (NTP) Port 123 / TCP
   14. Post Office Protocol 3 (POP3) Port 110 / TCP
   15. Session Initiation Protocol (SIP) Port 5060 / TCP, UDP
   16. Simple Mail Transfer Protocol (SMTP) Port 25 / TCP
   17. Simple Network Management Protocol (SNMP) Port 161 / TCP, UDP
   18. Socket Secure (SOCKS) Port 1080 / TCP
   19. Structured Query Language (SQL) Port 118 / TCP, UDP Port 156 / TCP, UDP
   20. Syslog Port 514 / UDP
   21. Telnet Port 23 / TCP
   22. Trivial File Transfer Protocol (TFTP) Port 69 / UDP
5. Review information systems quarterly to identify unnecessary and/or non-secure functions, ports, protocols, and services. Review and update the list of unauthorized software programs annually, at a minimum.
6. An information system shall prevent program execution in accordance with agency-defined policies regarding software program usage and restrictions, and/or rules authorizing the terms and conditions of software program usage.

#### Control Implementation Description:

*<<Description of control implementation>>*

### CM-8 Information System Component Inventory

#### North Carolina / NIST 800-53 Control Objective:

Agencies shall develop, document, and maintain an inventory of information system components. Agencies shall update the inventory of information system components as an integral part of component installations, removals, and information system updates. Agencies shall verify that all components within the authorization boundary of the information system are not duplicated in other information system component inventories. Component inventories shall include the following:

1. Accurately reflects the current information system,
2. Is consistent with the limit of the agency’s control of the information system,
3. All components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system,
4. Is at the level of granularity deemed necessary for tracking and reporting,
5. Includes information deemed necessary to achieve effective property accountability, for example, hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system / component owner, associated component configuration standard, software/firmware version information, and for a networked component/device, the machine name and network address,
6. Includes system and network diagrams,
7. Is available for review and audit by designated organizational officials,
8. Is included in property accountability information, a means for identifying by name and role individuals responsible for administering those components. A system containing restricted or highly restricted data may have multiple Data Owners, and/or System Administrators, but must have a single System Owner,
9. Includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory,
10. Review and update the information system component inventory through periodic manual inventory checks or a network monitoring tool that automatically maintains the inventory,
11. Includes all components that store, process, or transmit restricted or highly restricted data.

#### Control Implementation Description:

*<<Description of control implementation>>*

CM-8(3) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CM-8(3) Information System Component Inventory | Updates During Installation

#### North Carolina / NIST 800-53 Control Objective:

The agency:

(a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and

(b) Takes the following actions when unauthorized components are detected: disables network access by such components; isolates the components; notifies agency-defined personnel or roles]].

#### Control Implementation Description:

*<<Description of control implementation>>*

### CM-9 Configuration Management Plan

#### North Carolina / NIST 800-53 Control Objective:

The agency develops, documents, and implements a configuration management plan for the information system that:

1. Addresses roles, responsibilities, and configuration management processes and procedures;
2. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
3. Defines the configuration items for the information system and places the configuration items under configuration management; and
4. Protects the configuration management plan from unauthorized disclosure and modification.

#### Control Implementation Description:

*<<Description of control implementation>>*

### CM-10 Software Usage Restrictions

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Uses software and associated documentation in accordance with contract agreements and copyright laws;
2. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
3. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

#### Control Implementation Description:

NC DIT uses software in accordance with contract agreements and copyright laws. Agency tracks the use of software for servers with ADDM (Automatic Discovery and Data Mapping), and for desktop and laptop systems with SCCM (System Center Configuration Manager. Software installation is further enforced with restricted LDAP credentials and Access Control Lists. Compliance monitoring if enforced with aforementioned tools

### CM-11 User-Installed Software

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Establishes policies governing the installation of software by users;
2. Enforces software installation policies through automated methods, and
3. Monitors policy compliance quarterly, at a minimum.

#### Control Implementation Description:

*<<Description of control implementation>>*

## Contingency Planning (CP)

### CP-1 Contingency Planning Policy and Procedures

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops, documents, and disseminates to all State employees, contractors, vendors or other third-party users of IT resources
   1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
2. Reviews and updates the current:
   1. Contingency planning policy annually, at a minimum; and
   2. Contingency planning procedures [Assignment: organization-defined frequency].

#### Control Implementation Description:

*<<Description of control implementation>>*

### CP-2 Contingency Plan

#### North Carolina / NIST 800-53 Control Objective:

The State’s information assets must be available to authorized users when needed. Agencies are required to manage information technology risks appropriately as required in state and federal laws. Agencies must develop a contingency plan/disaster recovery plan for the recovery of information assets for which the State is named as owner for all known threats to availability, including natural disasters, accidents, malicious destruction, failures, and denial of services. Management shall coordinate contingency plan development with organizational elements responsible for formally documenting the Business Continuity (BC) & Disaster Recovery (DR) Plan that covers all of the agency’s essential and critical business processes and applications, and includes procedures or references to procedures to be used for the recovery of systems that perform the agency’s essential and critical business processes.

Agencies shall coordinate contingency plan development with agency divisions and groups responsible for related plans. Plans related to contingency plans for agency information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.

Agency plans must:

1. Be developed prior to implementation as part of the development life cycle for technology development or deployment by agency to address all production processing environments and assets.
2. Identify essential missions and business functions and associated contingency requirements.
3. Provide recovery time and recovery point objectives, restoration priorities, and metrics.
4. Identify contingency roles, responsibilities, assigned individuals with contact information.
5. Address eventual, full information asset restoration without deterioration of the security measures originally planned and implemented.
6. Be reviewed and approved by designated officials within the agency.
7. Be distributed to relevant system owners and stakeholders.
8. Coordinate contingency planning activities with incident handling activities.
9. Be revised to address changes to the organization, information asset, or environment of operation and problems encountered during contingency plan implementation, execution, or testing, and be communicated to relevant system owners and stakeholders.
10. Protect the contingency plan from unauthorized disclosure and modification.
11. Address the protection of the health and safety of the employees of the State of North Carolina.
12. Address the protection of assets of the State and minimize financial, legal and/or regulatory exposure.
13. Create crisis teams and response plans for threats and incidents.
14. Require that employees are made aware of their roles and responsibilities in the BC/DR Plan and in plan execution through training and awareness programs.
15. Coordination with Contingency Plan Administrators and the Operations Team must occur for all potential outages that may result in a failover situation.
16. Be submitted to the State CIO on an annual basis, and as otherwise requested by the State CIO.

Agencies shall plan for the resumption of essential missions and business functions within the agency-defined time period of contingency plan activation. Agencies may choose to carry out the contingency planning activities in this control enhancement as part of agency business continuity planning including, for example, as part of business impact analyses. The time period for resumption of essential mission/business functions will be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure.

Agencies may choose to carry out the contingency planning activities in this control enhancement as part of agency business continuity planning including, for example, as part of business impact analyses. Agencies shall identify critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that agency missions/business functions can continue to be conducted during contingency operations. In addition, the identification of critical information assets facilitates the prioritization of agency resources.

Critical information system assets include technical and operational aspects. Technical aspects include, for example, information technology services, information system components, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures). Agency program protection plans can provide assistance in identifying critical assets.

Application criticality has the following four categories (Definitions may be found in the Statewide Glossary of Information Technology Terms):

1. Statewide Critical
2. Department Critical
3. Program Critical
4. Non-Critical

#### Control Implementation Description:

*<<Description of control implementation>>*

### CP-3 Contingency Plan Training

#### North Carolina / NIST 800-53 Control Objective:

The agency provides contingency training to information system users consistent with assigned roles and responsibilities:

1. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility;
2. When required by information system changes; and
3. Annually thereafter.

#### Control Implementation Description:

*<<Description of control implementation>>*

### CP-4 Contingency Plan Testing and Exercises

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Tests the contingency plan for the information system annually using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan;
2. Reviews the contingency plan test results; and
3. Initiates corrective actions, if needed.

#### Control Implementation Description:

*<<Description of control implementation>>*

### CP-4(1) Contingency Plan Testing and Exercises | Coordinate with Other Related Plans

#### North Carolina / NIST 800-53 Control Objective:

The agency coordinates contingency plan testing with organizational elements responsible for related plans.

#### Control Implementation Description:

*<<Description of control implementation>>*

CP-6 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CP-6 Contingency Plan Alternate Storage Site

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and
2. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

#### Control Implementation Description:

*<<Description of control implementation>>*

CP-6(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CP-6(1) Contingency Plan Alternate Storage Site | Separation from Primary Site

#### North Carolina / NIST 800-53 Control Objective:

The agency identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

#### Control Implementation Description:

*<<Description of control implementation>>*

CP-6(3) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CP-6(3) Contingency Plan Alternate Storage Site | Accessibility

#### North Carolina / NIST 800-53 Control Objective:

The agency identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

#### Control Implementation Description:

*<<Description of control implementation>>*

CP-7 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CP-7 Contingency Plan Alternate Processing Site

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of information asset operations for essential missions/business functions within defined recovery times and recovery points when the primary processing capabilities are unavailable;
2. Ensures that equipment and supplies required to transfer, and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
3. Ensures that the alternate processing site provides information security safeguards equivalent to those of the primary site.

#### Control Implementation Description:

*<<Description of control implementation>>*

CP-7(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CP-7(1) Contingency Plan Alternate Processing Site | Separation from Primary Site

#### North Carolina / NIST 800-53 Control Objective:

The agency identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

#### Control Implementation Description:

*<<Description of control implementation>>*

CP-7(2) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CP-7(2) Contingency Plan Alternate Processing Site | Accessibility

#### North Carolina / NIST 800-53 Control Objective:

The agency identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

#### Control Implementation Description:

*<<Description of control implementation>>*

CP-7(3) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CP-7(3) Contingency Plan Alternate Processing Site | Priority of Service

#### North Carolina / NIST 800-53 Control Objective:

The agency develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

#### Control Implementation Description:

*<<Description of control implementation>>*

CP-8 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CP-8 Telecommunications Services

#### North Carolina / NIST 800-53 Control Objective:

Agencies shall do the following:

1. Establish alternate telecommunications services with telecommunication service providers that provide communications transmission services to maintain a state of readiness or to respond to and manage any event or crisis.
2. Communications transmission services must include necessary agreements to permit the resumption of information asset operations for essential missions and business functions within defined recovery time and recovery points when the primary telecommunications capabilities are unavailable.
3. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with agency availability requirements (including recovery time objectives).
4. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.
5. Consider the potential mission/business impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions.
6. Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.
7. This control is optional for LOW risk information systems.

#### Control Implementation Description:

*<<Description of control implementation>>*

### CP-9 Information System Backup

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Conducts backups of user-level information contained in the information system at a frequency that is consistent with agency defined recovery time and recovery point objectives;
2. Conducts backups of system-level information contained in the information system at a frequency that is consistent with agency defined recovery time and recovery point objectives;
3. Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and
4. Protects the confidentiality, integrity, and availability of backup information at storage locations.

#### Control Implementation Description:

*<<Description of control implementation>>*

CP-9(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CP-9(1) Information System Backup | Testing for Reliability / Integrity

#### North Carolina / NIST 800-53 Control Objective:

The agency tests backup information quarterly to verify media reliability and information integrity.

#### Control Implementation Description:

*<<Description of control implementation>>*

### CP-10 Information System Recovery and Reconstitution

#### North Carolina / NIST 800-53 Control Objective:

All State agencies must provide for the recovery and restoration of the agency’s mission essential function(s)/processes and/or critical business services to a known state after a disruption, compromise, or failure within defined RTO and RPO objectives. All plan activations must be documented and recorded, and post-activation reviews must be conducted to evaluate the effectiveness of the plan(s) and to update the plan(s) where necessary, and a formal report is provided to the State CIO within 30 days of post-activation review.

Agency information systems shall implement transaction recovery for systems that are transaction-based. Transaction-based information systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.

#### Control Implementation Description:

*<<Description of control implementation>>*

CP-11 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CP-11 Alternate Communications Protocols

#### North Carolina / NIST 800-53 Control Objective:

The information system provides the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of operations.

#### Control Implementation Description:

*<<Description of control implementation>>*

CP-12 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CP-12 Safe Mode

#### North Carolina / NIST 800-53 Control Objective:

The information system, when [Assignment: organization-defined conditions] are detected, enters a safe mode of operation with [Assignment: organization-defined restrictions of safe mode of operation].

#### Control Implementation Description:

*<<Description of control implementation>>*

CP-13 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### CP-13 Alternative Security Mechanisms

#### North Carolina / NIST 800-53 Control Objective:

The agency employs [Assignment: organization-defined alternative or supplemental security mechanisms] for satisfying [Assignment: organization-defined security functions] when the primary means of implementing the security function is unavailable or compromised.

#### Control Implementation Description:

*<<Description of control implementation>>*

## Identification and Authorization (IA)

### IA-1 Identification and Authentication Policy and Procedures

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops, documents, and disseminates to all covered personnel accessing or using IT resources;
   1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
2. Reviews and updates the current:
   1. Identification and authentication policy annually, at a minimum; and
   2. Identification and authentication procedures not defined, annually is implied.

#### Control Implementation Description:

*<<Description of control implementation>>*

### IA-2 Identification and Authentication Authorized Users

#### North Carolina / NIST 800-53 Control Objective:

Agency information systems and those operated on behalf of the agencies shall be configured to uniquely identify and authenticate users (or processes acting on behalf of users). Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal access).

1. System Owners shall not allow the use of shared accounts (credentials used by more than one individual) within their system unless a risk assessment determines that the confidentiality, integrity or availability of information or information systems is not at risk. The use of shared user accounts makes it difficult to uniquely identify individuals accessing an information system, as well as provide detailed accountability of user activity within an information system.
2. Identification and authentication mechanisms shall be implemented at the application level, as determined by a risk assessment, to provide increased security for the information system and the information processes. This shall be in addition to identifying and authenticating users at the information system level (e.g., when initially logging into a desktop, laptop, or mobile device).
3. Access to non-privileged accounts, privileged accounts, and all local accounts shall be authenticated through the use of passwords, personal identification numbers (PINs), tokens, biometrics, or in the case of multifactor authentication (MFA), some combination thereof. Note: See IA–5 - Authenticator Management for definitions of privileged and non-privileged accounts.
4. Agency information systems shall use MFA for the following conditions:
   1. Remote access to information systems using privileged accounts.
   2. Remote network access with privileged and non-privileged accounts for information systems that receive, process, store, or transmit federal tax information (FTI) or other highly restricted data.
   3. Remote access with privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access. The purpose of requiring a device that is separate from the information system gaining access for one of the factors during multifactor authentication is to reduce the likelihood of compromising authentication credentials stored on the system.
5. Agency information systems shall implement replay-resistant authentication mechanisms for network access to privileged accounts, if possible. Authentication processes resist replay attacks if it is impractical for an attacker to replay previous authentication messages and thus achieve unauthorized access. Replay-resistant techniques include, for example, protocols that use challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators (one-time passwords).

#### Control Implementation Description:

*<<Description of control implementation>>*

### IA-3 Device Identification and Authentication

#### North Carolina / NIST 800-53 Control Objective:

The information system uniquely identifies and authenticates unmanaged devices before establishing a location, network, or remote connection

#### Control Implementation Description:

*<<Description of control implementation>>*

### IA-4 Identifier Management

#### North Carolina / NIST 800-53 Control Objective:

The agency manages information system identifiers by:

1. Receiving authorization a designated agency representative (e.g., system administrator, technical lead or system owner) to assign an individual, group, role, or device identifier;
2. Selecting an identifier that identifies an individual, group, role, or device;
3. Assigning the identifier to the intended individual, group, role, or device;
4. Preventing reuse of identifiers for seven (7) years; and
5. Disabling identifiers after 120 days of inactivity, except as specifically exempted by agency management.

#### Control Implementation Description:

*<<Description of control implementation>>*

### IA-5 Authenticator Management

#### North Carolina / NIST 800-53 Control Objective:

Agencies shall manage information system authentication requirements. Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Agencies shall require the following:

1. Develop secure log-on procedures to be applied to all network components, operating systems, applications, and databases that implement a user identification and authentication mechanism. These procedures shall be designed to minimize the risk of unauthorized access.
2. Verify, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.
3. Establish initial authenticator content for authenticators defined by the agency.
4. Ensure that authenticators have sufficient strength of mechanism for their intended use.
5. Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
6. Change default content of authenticators, for example, the default password, prior to information system installation.
7. Require individuals to take, and have devices implement, specific security safeguards to protect authenticators from unauthorized disclosure and modification.
8. Change authenticators for group/role accounts when membership to those accounts changes.
9. Information systems shall display a message to users before or while they are prompted for their user identification and authentication credentials that warns against unauthorized or unlawful use. Refer to the Access Control policy AC-8 - System Use Notification for the standard State approved banner.
10. The log-on process should not be validated until all log-on data is input. Failing the process as each input field is completed will provide an attacker with information to further the attack.
11. Only generic “log-on failed” messages should be displayed if the user does not complete the log-on process successfully. Do not identify in the message whether the user identification, password, or other information is incorrect.
12. Agencies shall configure systems to limit the number of consecutive unsuccessful log-on attempts. If the number of consecutive unsuccessful log-on attempts exceeds the established limit, the configuration shall either force a time delay before further log-on attempts are allowed or shall disable the user account such that it can only be reactivated by a system or security administrator or an authorized service desk staff member.
13. For systems that store, transmit, or process FTI, the agency shall password-protect the system initialization (boot) settings.
14. All newly assigned passwords shall be changed the first time a user logs into the information system.
15. Where technically feasible, passwords shall be at least eight (8) characters long for access to all systems and applications.
16. Passwords shall have at least one numeric, at least one special character, and a mixture of at least one uppercase and at least one lowercase letter.
17. Passwords shall not contain number or character substitutes to create dictionary words (e.g., d33psl33p for deep sleep2).
18. Account passwords shall not traverse the network or be stored in clear text. All passwords stored shall be encrypted using FIPS-140-2 encryption.
19. Passwords shall not be inserted into email messages or other forms of electronic communication without proper encryption.
20. Information systems may allow the use of a temporary password for system logons as long as the temporary password is immediately changed to a permanent password upon the next logon attempt.
21. Passwords shall be different from all other accounts held by that user.
22. 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.
23. Passwords shall not be revealed to anyone, including supervisors, help desk personnel, security administrators, family members or co-workers.
24. Users shall enter passwords manually for each application or system, except for simplified/single sign-on systems that have been approved by the State CIO.
25. Passwords shall be changed whenever there is the suspicion or likelihood that the password or system is compromised.
26. Agencies shall validate the identity of an end user who requests a password reset. Initial passwords and subsequent password resets shall utilize a unique password for each user account.

#### Control Implementation Description:

*<<Description of control implementation>>*

### IA-6 Authenticator Feedback

#### North Carolina / NIST 800-53 Control Objective:

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

#### Control Implementation Description:

*<<Description of control implementation>>*

### IA-7 Cryptographic Module Authentication

#### North Carolina / NIST 800-53 Control Objective:

The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

#### Control Implementation Description:

*<<Description of control implementation>>*

### IA-8 Identification and Authentication (Non-Agency Users)

#### North Carolina / NIST 800-53 Control Objective:

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

#### Control Implementation Description:

*<<Description of control implementation>>*

IA-9 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### IA-9 Service Identification and Authentication

#### North Carolina / NIST 800-53 Control Objective:

The agency identifies and authenticates [Assignment: organization-defined information system services] using [Assignment: organization-defined security safeguards].

#### Control Implementation Description:

*<<Description of control implementation>>*

IA-10 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### IA-10 Adaptive Identification and Authentication

#### North Carolina / NIST 800-53 Control Objective:

The agency requires that individuals accessing the information system employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].

#### Control Implementation Description:

*<<Description of control implementation>>*

IA-11 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### IA-11 Re-authentication

#### North Carolina / NIST 800-53 Control Objective:

The agency requires users and devices to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].

#### Control Implementation Description:

*<<Description of control implementation>>*

## Incident Response (IR)

### IR-1 Incident Response Policy and Procedures

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops, documents, and disseminates to All covered personnel that utilize IT resources;
   1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
2. Reviews and updates the current:
   1. Incident response policy annually, at a minimum; and
   2. Incident response procedures [Assignment: organization-defined frequency].

#### Control Implementation Description:

*<<Description of control implementation>>*

### IR-2 Incident Response Plan Training

#### North Carolina / NIST 800-53 Control Objective:

The agency provides incident response training to information system users consistent with assigned roles and responsibilities:

1. Prior to assuming an incident response role or responsibility;
2. When required by information system changes; and
3. Annually thereafter.

#### Control Implementation Description:

*<<Description of control implementation>>*

IR-3 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### IR-3 Incident Response Plan Testing

#### North Carolina / NIST 800-53 Control Objective:

The agency tests the incident response capability for the information system at least annually using tabletop exercises to determine the incident response effectiveness and documents the results.

#### Control Implementation Description:

*<<Description of control implementation>>*

MP-3 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### IR-3(2) Incident Response Plan Testing | Coordination With Related Plans

#### North Carolina / NIST 800-53 Control Objective:

The agency coordinates incident response testing with organizational elements responsible for related plans.

#### Control Implementation Description:

*<<Description of control implementation>>*

### IR-4 Incident Handling

#### North Carolina / NIST 800-53 Control Objective:

The State shall protect technology resources by conducting proper investigations:

1. The IRM, acting on behalf of the SCIO, shall evaluate the proper response to all information technology security incidents reported to the agency.
2. The IRM shall work with agencies to decide what resources, including law enforcement, are required to best respond to and mitigate the incident.
3. After the initial reporting and/or notification, agency management shall review and reassess the level of impact that the incident created.
4. The IRM shall coordinate incident handling activities with contingency planning activities.
5. An investigation into an information technology security incident must identify its cause, if possible, and appraise its impact on systems and data. The extent of damage must be determined and course of action planned and communicated to the appropriate parties.
6. Agencies shall investigate information system failures to determine whether the failure was caused by malicious activity or by some other means (i.e., hardware or software failure).
7. If any suspicious activities are detected, responsible personnel within the affected agency shall be notified to ensure that proper action is taken.
8. Agencies shall establish controls to protect data integrity and confidentiality during investigations of information technology security incidents. Controls shall either include dual-control procedures or segregation of duties to ensure fraudulent activities requiring collusion do not occur.
9. Evidence of or relating to an information technology security breach shall be collected and preserved in a manner that is in accordance with State and federal requirements.
10. The collection process shall include a document trail, the chain of custody for items collected, and logs of all evidence-collecting activities to ensure the evidence is properly preserved for any legal actions that may ensue as a result of the incident.
11. Any system, network, or security administrator who observes an intruder on the State network or system shall take appropriate action to terminate the intruder’s access. (Intruder can mean a hacker, botnet, malware, etc.)
12. In the event of an active incident, agency management has the authority to decide whether to continue collecting evidence or to restrict physical and logical access to the system involved in the incident. Note: It may be necessary to isolated from the network until the extent of the damage can be assessed.
13. When dealing with a suspected incident, agencies shall do the following:
    1. Make an image of the system (including volatile memory, if possible) so that original evidence may be preserved.
    2. Make copies of all audit trail information such as system logs, network connections (including IP addresses, TCP/UDP ports, length, and number), super user history files, etc.
    3. Take steps to preserve and secure the trail of evidence.
14. The agency’s CIO or his/her designee will determine if other agencies, departments, or personnel need to become involved in resolution of the incident. Agencies shall consider coordinating IR activities with external organizations, such as the OSA, OSHR, SBI, or the FBI.
15. Agencies shall require all personnel directly involved with incident handling sign a Non-Disclosure Agreement (NDA).
16. Agencies shall discuss incident details only on a need-to-know basis with authorized personnel.
17. When responding to a malware threat, agencies shall perform the following tasks:
    1. Verify threats to rule out the possibility of a hoax before notifying others
    2. Identify personnel responsible for mitigation of malware threats
    3. Have internal escalation procedures and severity levels
    4. Have processes to identify, contain, eradicate, and recover from malware events
    5. Have a contact list of antivirus software vendors
18. Agencies may utilize the following for guidance regarding incident handling:
    1. NIST SP 800-36, Guide to Selecting Information Technology Security Products;
    2. NIST SP 800-61, Computer Security Incident Handling Guide, Revision 2;
    3. NIST SP 800-83, Guide to Malware Prevention and Incident Handling for Desktops and Laptops, Revision 1;
    4. NIST SP 800-86, Guide for Integrating Forensic Techniques into Incident Response;
    5. NIST SP 800-92, Guide to Information Security Log Management;
    6. NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS);
    7. NIST SP 800-101, Guidelines on Mobile Device Forensics, Revision 1; and
    8. Other appropriate guidance, as necessary.
19. Agencies shall activate and implement a security incident handling capability during all stages of the NIST incident response life cycle (See Figure 1 in Incident Response policy), including the following:
    1. Preparation
    2. Detection and Analysis
    3. Containment, Eradication, and Recovery
    4. Post-Incident Activities
20. All agencies shall ensure the integrity of information systems incident investigations by having the records of such investigations audited by qualified individuals as determined by agency management.
21. All agencies shall maintain records of information security breaches and the remedies used for resolution as references for evaluating any future security breaches. The information shall be logged and maintained in such a location that it cannot be altered by others. The recorded events shall be studied and reviewed regularly as a reminder of the lessons learned.
22. The agency/department IT manager and/or incident response coordinator shall determine the criticality of an incident (see IR-6 for severity levels).
23. Agencies shall enact automated processes for the purpose of correlating security events, e.g. Security Information and Event Management (SIEM) technology.
24. Lessons learned from incident handling activities shall be incorporated into incident response procedures, training, and testing/exercises, and implements the resulting changes.
25. Agencies shall create processes to provide information for the enhancement of organizational and Agency information security awareness programs and incident response programs.

#### Control Implementation Description:

*<<Description of control implementation>>*

### IR-5 Incident Monitoring

#### North Carolina / NIST 800-53 Control Objective:

The agency tracks and documents information system security incidents.

#### Control Implementation Description:

*<<Description of control implementation>>*

### IR-6 Incident Reporting

#### North Carolina / NIST 800-53 Control Objective:

To increase effectiveness in assessing threat levels and detecting patterns or trends in regard to information technology security incidents through proper documentation all computer security incidents. Security incidents, for example, suspicious events (e.g. insider threat), software errors or weaknesses, system vulnerabilities associated with security incidents (e.g. Ransomware), and lost or stolen State computer equipment, shall be reported immediately to the agency management.

1. Agencies 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. Agencies shall report incidents to the ESRMO by one of the following methods:
   1. Contact DIT Customer Support Center 800-722-3946
   2. ii. Use the incident reporting website https://it.nc.gov/cybersecurity-situation-report.
   3. iii. Contact a member of the ESRMO staff directly by phone or email security@its.nc.gov.
2. For incidents involving FTI, agencies shall report incidents no later than twenty-four (24) hours after identification of a possible issue involving FTI. Refer to IRS 1075 Section 10.0, Reporting Improper Inspections or Disclosures, for more information on incident reporting requirements.
3. For reporting security incidents to outside authorities, agencies shall do the following:
   1. Agencies shall coordinate with ESRMO in accordance with the State’s Incident Response Plan, applicable state laws, procedures, and agreements that require reporting to the Department of Justice, the State Bureau of Investigation, and the Office of the State Auditor. Agencies shall report all security incidents to the ESRMO when reported to an outside entity.
   2. Agencies shall notify the Social Security Administration (SSA) Regional Office and their SSA Systems Security Contact within one (1) hour of suspecting loss if a privacy or security incident involves the unauthorized disclosure of Social Security data. If the security incident is related to the State Transmission/Transfer Component (STC) and the agency is unable to notify the SSA Regional Office or the SSA Systems Security Contact within 1 hour, the STC must report the incident by contacting SSA’s National Network Service Center (NNSC) at 1-877-697-4889. Refer to the statewide Privacy Policy, NC-SEC-318-00, for additional guidance.
   3. If a security incident involves the possible breach of FTI, the agency must contact the appropriate special agent-in-charge, the Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguards immediately, but no later than twenty-four (24) hours after identification.
   4. Agencies shall notify consumers in the event of a security breach resulting in the unauthorized release of unencrypted or un-redacted records or data containing personal information with corresponding names. Note: The acquisition of encrypted data is only a breach if a confidential process or key needed to unlock the data is also breached, or if the data is encrypted by an unauthorized or malicious process, such as ransomware.
   5. The agency CIO and/or his/her designee shall manage the dissemination of incident information to other participants, for example law enforcement or the press. Public release of information concerning a security incident shall be coordinated through the agency’s CIO, the Incident Response Team (IRT), and the agency’s Public Information Officer (PIO).
4. Information recorded in regard to information technology security breaches shall cover the following at a minimum:
   1. Identify the current level of impact on agency functions or services (Functional Impact).
   2. Identify the type of information lost, compromised, or corrupted (Information Impact).
   3. Estimate the scope of time and resources needed to recover from the incident (Recoverability).
   4. Identify when the activity was first detected and when corrective actions were implemented.
   5. Identify the number of systems, records, and users impacted.
   6. Identify the network location of the observed activity.
   7. Identify point of contact information for additional follow-up.
   8. Identify the attack vector(s) that led to the incident.
   9. The method of breach detection and incident response actions
   10. Provide any indicators of compromise, including signatures or detection measures developed in relationship to the incident.
   11. Provide any mitigation activities undertaken in response to the incident.

#### Control Implementation Description:

*<<Description of control implementation>>*

### IR-7 Incident Response Assistance

#### North Carolina / NIST 800-53 Control Objective:

The agency provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

#### Control Implementation Description:

*<<Description of control implementation>>*

### IR-8 Incident Response Plan

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops an incident response plan that:
   1. Provides the organization with a roadmap for implementing its incident response capability;
   2. Describes the structure and organization of the incident response capability;
   3. Provides a high-level approach for how the incident response capability fits into the overall organization;
   4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
   5. Defines reportable incidents;
   6. Provides metrics for measuring the incident response capability within the organization;
   7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
   8. Is reviewed and approved by designated State or agency officials;
2. Distributes copies of the incident response plan to State and agency identified incident response personnel,;
3. Reviews the incident response plan annually;
4. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
5. Communicates incident response plan changes to identified State and agency officials; and
6. Protects the incident response plan from unauthorized disclosure and modification.

#### Control Implementation Description:

*<<Description of control implementation>>*

IR-9 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### IR-9 Information Spillage Response

#### North Carolina / NIST 800-53 Control Objective:

The agency responds to information spills by:

1. Identifying the specific information involved in the information system contamination;
2. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;
3. Isolating the contaminated information system or system component;
4. Eradicating the information from the contaminated information system or component;
5. Identifying other information systems or system components that may have been subsequently contaminated; and
6. Performing other [Assignment: organization-defined actions].

#### Control Implementation Description:

*<<Description of control implementation>>*

IR-10 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### IR-10 Integrated Information Security Analysis Team

#### North Carolina / NIST 800-53 Control Objective:

The agency establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.

#### Control Implementation Description:

*<<Description of control implementation>>*

## Maintenance (MA)

### MA-1 System Maintenance Policy and Procedures

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops, documents, and disseminates to all covered personnel involved in the maintenance of information systems and supporting infrastructure:
   1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and
2. Reviews and updates the current:
   1. System maintenance policy annually, at a minimum; and
   2. System maintenance procedures [Assignment: organization-defined frequency.

#### Control Implementation Description:

*<<Description of control implementation>>*

### MA-2 Controlled Maintenance

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
2. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
3. Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
4. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
5. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
6. f. Includes date and time of information system security maintenance, name of the individual performing the information system security maintenance, name of escort, if necessary, description of the information system security maintenance performed and list of equipment removed or replaced (including identification numbers, if applicable).] in organizational maintenance records.

#### Control Implementation Description:

*<<Description of control implementation>>*

MA-3 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### MA-3 Maintenance Tools

#### North Carolina / NIST 800-53 Control Objective:

The agency approves, controls, and monitors information system maintenance tools.

#### Control Implementation Description:

*<<Description of control implementation>>*

MA-3(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### MA-3(1) Maintenance Tools | Inspect Tools

#### North Carolina / NIST 800-53 Control Objective:

The agency inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

#### Control Implementation Description:

*<<Description of control implementation>>*

MA-3(2) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### MA-3(2) Maintenance Tools | Inspect Media

#### North Carolina / NIST 800-53 Control Objective:

The agency checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

#### Control Implementation Description:

*<<Description of control implementation>>*

### MA-4 Nonlocal Maintenance

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Approves and monitors nonlocal maintenance and diagnostic activities;
2. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
3. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
4. Maintains records for nonlocal maintenance and diagnostic activities; and
5. Terminates session and network connections when nonlocal maintenance is completed.

#### Control Implementation Description:

*<<Description of control implementation>>*

MA-4 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### MA-4(2) Nonlocal Maintenance | Document Nonlocal Maintenance

#### North Carolina / NIST 800-53 Control Objective:

The agency documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

#### Control Implementation Description:

*<<Description of control implementation>>*

### MA-5 Maintenance Personnel

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
2. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
3. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

#### Control Implementation Description:

*<<Description of control implementation>>*

MA-6 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### MA-6 Timely Maintenance

#### North Carolina / NIST 800-53 Control Objective:

Agencies shall perform preventative information system security maintenance support for the purpose of maintaining equipment and facilities in satisfactory operating conditions.

1. Predictive maintenance, or condition-based maintenance shall be performed by conducting periodic or continuous (online) equipment condition monitoring.
2. Where feasible, automated mechanisms should be used to transfer predictive maintenance data to a computerized maintenance management system.
3. This control is optional for LOW risk information systems.

#### Control Implementation Description:

*<<Description of control implementation>>*

## Media Protection (MP)

### MP-1 Media Protection Policy and Procedures

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops, documents, and disseminates to all covered personnel involved in the handling of media:
   1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
2. Reviews and updates the current:
   1. Media protection policy at a minimum of every year or when there is a significant change that may impact the security posture of the data and / or system, and
   2. Media protection procedures [Assignment: organization-defined frequency].

#### Control Implementation Description:

*<<Description of control implementation>>*

### MP-2 Media Access

#### North Carolina / NIST 800-53 Control Objective:

The agency restricts access to all digital and non-digital media to authorized individuals only.

#### Control Implementation Description:

*<<Description of control implementation>>*

MP-3 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### MP-3 Media Marking

#### North Carolina / NIST 800-53 Control Objective:

1. All data must be labeled to reflect its classification. Recipients of information must maintain an assigned label and protect the information.
2. If a storage volume or information source contains multiple classifications, then the highest classification shall appear on the label. Data labeling may be automated where possible or done manually.
3. If known, the applicable statute shall be cited on the label. For example, “Low Risk / Restricted per N.C.G.S. 132-6.1(c)”.
4. Agencies must label removable media (CDs, DVDs, diskettes, magnetic tapes, external hard drives and flash drives) and information system output containing FTI (reports, documents, data files, back-up tapes) indicating “Federal Tax Information”.
5. The table associated with this control in the Media Protection policy summarizes labeling requirements for different classes of data.
6. This control is optional for LOW risk information systems.

#### Control Implementation Description:

*<<Description of control implementation>>*

MP-4 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### MP-4 Media Storage

#### North Carolina / NIST 800-53 Control Objective:

Agencies shall ensure the proper storage of data and information files for which they are responsible.

1. Stored data shall be protected and backed up so that a restoration can occur in the event of accidental or unauthorized deletion or misuse.
2. Agencies shall also meet all applicable statutory and regulatory requirements for data retention, destruction, and protection.
3. Agencies shall protect the State’s information and comply with the agency records retention policy or the General Schedule for State Agency Records, Information Technology Records.
4. Agencies shall ensure encryption keys are properly stored (separate from data) and available, if needed, for later decryption. When using encryption to protect data, agencies shall follow the statewide information security standard for encryption.
5. Agencies shall establish change management procedures for the emergency amendment of data that occurs outside normal software functions and procedures.
6. All emergency amendments or changes shall be properly documented and approved and shall meet all applicable statutory and regulatory requirements.
7. Agencies shall physically control and securely store media containing FTI.
8. Agencies shall protect information system media until the media is destroyed or sanitized using approved equipment, techniques, and procedures.
9. Agencies shall encrypt data stored on secondary storage devices (devices that retain copies of data stored on primary data storage devices, i.e. backups) as required for the protection of the highest level of information contained therein.
10. Agencies shall keep stored public data to a minimum of what is necessary to adequately perform their business functions. Sensitive or confidential data that is not needed for normal business functions, such as the full contents of a credit card magnetic strip or a credit card PIN, should not be stored. Agencies should consider implementing a process (automatic or manual) to remove, at least quarterly, stored confidential data, like cardholder data, that exceeds the requirements defined in the agency’s data retention policy.
11. This control is optional for LOW risk information systems.

**Media Archival**

Agencies shall consult with the NC Department of Natural and Cultural Resources, Government Records Section, to select archival media that will protect the integrity of the data stored on those media for as long as the data are archived. In addition, the following requirements must be met:

1. When archiving data associated with legacy systems, agencies should plan to provide a method of accessing those data.
2. Classification of the back-up media so the sensitivity of the data can be determined.
3. Storage of media back-ups in a secure location, preferably an off-site facility.
4. All back-up media are physically secured from theft and destruction.
5. Migrating data to another system or archiving data shall be in accordance with applicable records management regulations and policies for potential future access.

#### Control Implementation Description:

*<<Description of control implementation>>*

MP-5 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### MP-5 Media Transport

#### North Carolina / NIST 800-53 Control Objective:

All users must observe the requirements for transferring or communicating information based on its sensitivity, which are defined in the table in the Media Protection policy. Data stewards, or their assigned representatives, may designate additional controls to further restrict access to, or to further protect, information:

1. Access to data shall be granted only after a business need has been demonstrated and approved by the data steward.
2. Agencies must use transmittals or an equivalent documented tracking method to ensure FTI and other restricted or highly restricted data reaches its intended destination.
3. Media are transported by secured courier or other delivery method that can be accurately tracked.
4. Management approval shall be obtained before moving any media from a secure area.
5. Inventory logs of all media, shall be properly maintained, and an inventory of all media logs, shall be performed at least annually.

Refer also to table in the MP-5 entry of the Media Protection policy.

#### Control Implementation Description:

*<<Description of control implementation>>*

### MP-6 Media Sanitization

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Sanitizes media prior to disposal, release out of organizational control, or release for reuse using in accordance with the National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1, Guidelines for Media Sanitization; and
2. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

#### Control Implementation Description:

*<<Description of control implementation>>*

### MP-7 Media Use

#### North Carolina / NIST 800-53 Control Objective:

The agency restricts the use of non-state owned media and devices on information systems or system components.

#### Control Implementation Description:

*<<Description of control implementation>>*

MP-7(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### MP-7(1) Media Use | Prohibit Use Without Owner

#### North Carolina / NIST 800-53 Control Objective:

The agency prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

#### Control Implementation Description:

*<<Description of control implementation>>*

MP-8 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### MP-8 Media Downgrading

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Establishes [Assignment: organization-defined information system media downgrading process] that includes employing downgrading mechanisms with [Assignment: organization-defined strength and integrity];
2. Ensures that the information system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information;
3. Identifies [Assignment: organization-defined information system media requiring downgrading]; and
4. Downgrades the identified information system media using the established process.

#### Control Implementation Description:

*<<Description of control implementation>>*

## Physical and Environmental Protection (PE)

### PE-1 Physical and Environmental Protection Policy and Procedures

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops, documents, and disseminates to all covered personnel involved in the maintenance of information systems and supporting infrastructure:
   1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and
2. Reviews and updates the current:
   1. Physical and environmental protection policy annually; and
   2. Physical and environmental protection procedures [Assignment: organization-defined frequency].

#### Control Implementation Description:

*<<Description of control implementation>>*

### PE-2 Physical Access Authorizations

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
2. Issues authorization credentials for facility access;
3. Reviews the access list detailing authorized facility access by individuals quarterly; and
4. Removes individuals from the facility access list when access is no longer required.

#### Control Implementation Description:

*<<Description of control implementation>>*

### PE-3 Physical Access Control

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Enforces physical access authorizations at entry/exit points to the facility where the information systems that receive, process, store or transmit restricted or highly restricted data resides by;
   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress/egress to the facility using physical access control systems/devices or guards;
2. Maintains physical access audit logs for agency-defined entry/exit points];
3. Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible;
4. Escorts visitors and monitors visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and monitoring];
5. Secures keys, combinations, and other physical access devices;
6. Inventories [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and
7. Changes combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

#### Control Implementation Description:

*<<Description of control implementation>>*

PE-4 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### PE-4 Access Control for Transmission Medium

#### North Carolina / NIST 800-53 Control Objective:

The agency controls physical access to information system distribution and transmission lines within agency facilities.

#### Control Implementation Description:

*<<Description of control implementation>>*

PE-5 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### PE-5 Access Control for Output Devices

#### North Carolina / NIST 800-53 Control Objective:

The agency controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

#### Control Implementation Description:

*<<Description of control implementation>>*

### PE-6 Monitoring Physical Access

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
2. Reviews physical access logs at least semi-annually and upon occurrence of apparent security violations; and
3. Coordinates results of reviews and investigations with the organizational incident response capability.

#### Control Implementation Description:

*<<Description of control implementation>>*

PE-6(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### PE-6(1) Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment

#### North Carolina / NIST 800-53 Control Objective:

The agency monitors physical intrusion alarms and surveillance equipment.

#### Control Implementation Description:

*<<Description of control implementation>>*

### PE-8 Visitor Access Records

#### North Carolina / NIST 800-53 Control Objective:

Agencies shall actively monitor the security access logs of areas housing information technology equipment:

1. Visitor access records for agency owned computing facilities shall address the following requirements:
   1. Name and organization of the person visiting
   2. Signature of the visitor
   3. Picture ID has been verified, and by whom, i.e. guard’s initials
   4. Date of access
   5. Time of entry and departure
   6. Purpose of visit
   7. Name of person visited
   8. The visitor access records shall be reviewed at least semi-annually
2. Visitor access records for facilities housing FTI shall be maintained for five (5) years. All other facilities access records shall comply with the State’s records retention policies.

#### Control Implementation Description:

*<<Description of control implementation>>*

PE-9 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### PE-9 Power Equipment and Cabling

#### North Carolina / NIST 800-53 Control Objective:

The agency protects power equipment and power cabling for the information system from damage and destruction.

#### Control Implementation Description:

*<<Description of control implementation>>*

PE-10 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### PE-10 Emergency Shutoff

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
2. Places emergency shutoff switches or devices in a visible location and are clearly labeled to facilitate safe and easy access for personnel; and
3. Protects emergency power shutoff capability from unauthorized activation.

#### Control Implementation Description:

*<<Description of control implementation>>*

PE-11 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### PE-11 Emergency Power

#### North Carolina / NIST 800-53 Control Objective:

The agency provides a short-term uninterruptible power supply to facilitate both: an orderly shutdown of the information system; transition of the information system to long-term alternate power in the event of a primary power source loss.

#### Control Implementation Description:

*<<Description of control implementation>>*

### PE-12 Emergency Lighting

#### North Carolina / NIST 800-53 Control Objective:

The agency employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

#### Control Implementation Description:

*<<Description of control implementation>>*

### PE-13 Fire Protection

#### North Carolina / NIST 800-53 Control Objective:

The agency employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

#### Control Implementation Description:

*<<Description of control implementation>>*

PE-13(3) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### PE-13(3) Fire Protection | Automatic Fire Suppression

#### North Carolina / NIST 800-53 Control Objective:

The agency employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

#### Control Implementation Description:

*<<Description of control implementation>>*

### PE-14 Temperature and Humidity Controls

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Maintains temperature and humidity levels within the facility where the information system resides at agency-defined acceptable levels; and
2. Monitors temperature and humidity levels continuously.

#### Control Implementation Description:

*<<Description of control implementation>>*

### PE-15 Water Damage Protection

#### North Carolina / NIST 800-53 Control Objective:

The agency protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

#### Control Implementation Description:

*<<Description of control implementation>>*

### PE-16 Delivery and Removal

#### North Carolina / NIST 800-53 Control Objective:

The agency authorizes, monitors, and controls all types of information system components and packages entering and exiting the facility and maintains records of those items.

#### Control Implementation Description:

*<<Description of control implementation>>*

PE-17 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### PE-17 Alternate Work Site

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. shall provide readily available alternate work locations as part of contingency operations such as governmental offices, commercial locations or employee homes;
2. Assess as feasible, the effectiveness of security controls at alternate work sites; and
3. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

#### Control Implementation Description:

*<<Description of control implementation>>*

PE-18 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### PE-18 Location of Information System Components

#### North Carolina / NIST 800-53 Control Objective:

The agency positions information system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.

#### Control Implementation Description:

*<<Description of control implementation>>*

PE-19 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### PE-19 Information Leakage

#### North Carolina / NIST 800-53 Control Objective:

The agency protects the information system from information leakage due to electromagnetic signals emanations.

#### Control Implementation Description:

*<<Description of control implementation>>*

PE-20 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### PE-20 Asset Monitoring and Tracking

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Employs [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas]; and
2. Ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

#### Control Implementation Description:

*<<Description of control implementation>>*

## Planning (PL)

PL-1 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### PL-1 Security Planning Policy and Procedures

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops, documents, and disseminates to all covered personnel:
   1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and
2. Reviews and updates the current:
   1. Security planning policy annually, at least; and
   2. Security planning procedures [Assignment: organization-defined frequency].

#### Control Implementation Description:

*<<Description of control implementation>>*

PL-2 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### PL-2 System Security Plan

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops a security plan for the information system that:
   1. Is consistent with the agency’s enterprise architecture;
   2. Explicitly defines the authorization boundary for the system;
   3. Describes the operational context of the information system in terms of missions and business processes;
   4. Provides the security categorization of the information system including supporting rationale;
   5. Describes the operational environment for the information system and relationships with or connections to other information systems;
   6. Provides an overview of the security requirements for the system;
   7. Identifies any relevant overlays, if applicable;
   8. Describes the security controls in place or planned for
   9. meeting those requirements including a rationale for the tailoring decisions; and
   10. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
2. Distributes copies of the security plan and communicates subsequent changes to the plan to appropriate agency personnel;
3. Reviews the security plan for the information system on an annual basis;
4. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
5. Protects the security plan from unauthorized disclosure and modification.

#### Control Implementation Description:

*<<Description of control implementation>>*

PL-2(3) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### PL-2(3) System Security Plan | Plan / Coordinate with Other Organizational Entities

#### North Carolina / NIST 800-53 Control Objective:

The agency plans and coordinates security-related activities affecting the information system with other agency entities (departments, divisions, management, etc.) before conducting such activities in order to reduce the impact on other organizational entities.

#### Control Implementation Description:

*<<Description of control implementation>>*

### PL-4 Rules of Behavior

#### North Carolina / NIST 800-53 Control Objective:

The State:

1. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
2. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
3. Reviews and updates the rules of behavior annually, or whenever a significant change to the information system occurs; and
4. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

#### Control Implementation Description:

*<<Description of control implementation>>*

PL-4(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### PL-4(1) Rules of Behavior | Social Media and Networking Restrictions

#### North Carolina / NIST 800-53 Control Objective:

The agency includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

#### Control Implementation Description:

*<<Description of control implementation>>*

PL-7 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### PL-7 Security Concept of Operations

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the agency intends to operate the system from the perspective of information security; and
2. Reviews and updates the CONOPS [Assignment: organization-defined frequency].

#### Control Implementation Description:

*<<Description of control implementation>>*

### PL-8 Information Security Architecture

#### North Carolina / NIST 800-53 Control Objective:

Agencies shall develop an information security architecture as a requirement for the project review process. This information is captured within the Statewide Architectural Framework, which can be found at <https://it.nc.gov/services/it-architecture/statewide-architecture-framework>. Information security architecture shall include the following:

1. Description of the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.
2. Description of how the information security architecture is integrated into and supports the enterprise architecture.
3. Description of any information security assumptions about, and dependencies on, external services.
4. An annual review and update of the information security architecture to reflect changes in the enterprise architecture.

#### Control Implementation Description:

*<<Description of control implementation>>*

PL-9 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### PL-9 Information Security Architecture

#### North Carolina / NIST 800-53 Control Objective:

The organization centrally manages [Assignment: organization-defined security controls and related processes].

#### Control Implementation Description:

*<<Description of control implementation>>*

## Personnel Security (PS)

### PS-1 Personnel Security Policy and Procedures

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops, documents, and disseminates to all covered personnel involved in the maintenance of information systems and supporting infrastructure:
   1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
2. Reviews and updates the current:
   1. Personnel security policy annually; and
   2. Personnel security procedures [Assignment: organization-defined frequency].

#### Control Implementation Description:

*<<Description of control implementation>>*

### PS-2 Position Risk Designation

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Assigns a risk designation to all organizational positions;
2. Establishes screening criteria for individuals filling those positions; and
3. Reviews and updates position risk designations annually.

#### Control Implementation Description:

*<<Description of control implementation>>*

### PS-3 Personnel Screening

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Screens individuals prior to authorizing access to the information system; and
2. Rescreens individuals as needed and in compliance with the State’s personnel screening procedures. Recruitment procedures may be found in the State Human Resources Manual.

#### Control Implementation Description:

*<<Description of control implementation>>*

### PS-4 Personnel Termination

#### North Carolina / NIST 800-53 Control Objective:

The agency, upon termination of individual employment:

1. Disables information system access immediately;
2. Terminates/revokes any authenticators/credentials associated with the individual;
3. Conducts exit interviews that include a discussion of non-disclosure agreements and potential limitations of future employment;
4. Retrieves all security-related organizational information system-related property;
5. Retains access to organizational information and information systems formerly controlled by terminated individual; and
6. Notifies the agency’s help desk, security office, security guard, and the individuals manager] immediately upon notification of termination.

#### Control Implementation Description:

*<<Description of control implementation>>*

### PS-5 Personnel Transfer

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
2. Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];
3. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
4. Notifies appropriate agency personnel as required.

#### Control Implementation Description:

*<<Description of control implementation>>*

### PS-6 Access Agreements

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops and documents access agreements for organizational information systems;
2. Reviews and updates the access agreements annually; and
3. Ensures that individuals requiring access to organizational information and information systems:
   1. Sign appropriate access agreements prior to being granted access; and
   2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or at least annually.

#### Control Implementation Description:

*<<Description of control implementation>>*

### PS-7 Third-Party Personnel Security

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
2. Requires third-party providers to comply with personnel security policies and procedures established by the agency;
3. Documents personnel security requirements;
4. Requires third-party providers to notify The Agency Security Liason or other designated agency personnel of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges as soon as transfers or terminations are known; and
5. Monitors provider compliance.

#### Control Implementation Description:

*<<Description of control implementation>>*

### PS-8 Personnel Sanctions

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
2. Notifies OSHR immediately when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

#### Control Implementation Description:

*<<Description of control implementation>>*

## Risk Assessment (RA)

### RA-1 Risk Assessment Policy and Procedures

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops, documents, and disseminates to all covered personnel that are included in IT risk assessment activities:
   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
2. Reviews and updates the current:
   1. Risk assessment policy annually; and
   2. Risk assessment procedures [Assignment: organization-defined frequency].

#### Control Implementation Description:

*<<Description of control implementation>>*

### RA-2 Security Categorization

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Categorizes information and the information system in accordance with applicable federal laws,
2. Executive Orders, directives, policies, regulations, standards, and guidance;
3. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
4. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

#### Control Implementation Description:

*<<Description of control implementation>>*

### RA-3 Risk Assessment

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the
2. unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
3. Documents risk assessment results are provided to the ESRMO
4. Reviews risk assessment results within thirty (30) days of completion;
5. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and
6. Updates the risk assessment annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

#### Control Implementation Description:

*<<Description of control implementation>>*

### RA-5 Vulnerability Scanning

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Scans for vulnerabilities in the information system and hosted applications performed at least every seven (7) days and when new vulnerabilities potentially affecting the system/applications are identified and reported;
2. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
   1. Enumerating platforms, software flaws, and improper configurations;
   2. Formatting checklists and test procedures; and
   3. Measuring vulnerability impact;
3. Analyzes vulnerability scan reports and results from security control assessments;
4. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and
5. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

#### Control Implementation Description:

*<<Description of control implementation>>*

RA-5(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### RA-5(1) Vulnerability Scanning | Update Tool Capability

#### North Carolina / NIST 800-53 Control Objective:

The agency employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

#### Control Implementation Description:

*<<Description of control implementation>>*

RA-5(2) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### RA-5(2) Vulnerability Scanning | Update by Frequency

#### North Carolina / NIST 800-53 Control Objective:

The agency updates the information system vulnerabilities scanned prior to a new scan or when new vulnerabilities are identified and reported.

#### Control Implementation Description:

*<<Description of control implementation>>*

RA-5(5) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### RA-5(5) Vulnerability Scanning | Privileged Access

#### North Carolina / NIST 800-53 Control Objective:

The information system implements privileged access authorization to an information system for vulnerability scanning activities.

#### Control Implementation Description:

*<<Description of control implementation>>*

RA-6 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### RA-6 Technical Surveillance Countermeasures Survey

#### North Carolina / NIST 800-53 Control Objective:

The agency employs a technical surveillance countermeasures survey at [Assignment: organization-defined locations] [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined events or indicators occur]].

#### Control Implementation Description:

*<<Description of control implementation>>*

## System and Services Acquisition (SA)

### SA-1 SA Policy

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops, documents, and disseminates to all covered personnel in the acquisition, development or operation of information systems and supporting infrastructure:
   1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and
2. Reviews and updates the current:
   1. System and services acquisition policy [Assignment: organization-defined frequency]; and
   2. System and services acquisition procedures [Assignment: organization-defined frequency].

#### Control Implementation Description:

*<<Description of control implementation>>*

### SA-2 Allocation of Resources

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Determines information security requirements for the information system or information system
2. service in mission/business process planning;
3. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
4. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SA-3 System Development Life Cycle

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Manages the information system using agency-defined system development life cycle that incorporates information security considerations;
2. Defines and documents information security roles and responsibilities throughout the system development life cycle;
3. Identifies individuals having information security roles and responsibilities; and
4. Integrates the organizational information security risk management process into system development life cycle activities.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SA-4 Acquisition Process

#### North Carolina / NIST 800-53 Control Objective:

The agency includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

Security functional requirements shall include security capabilities, security functions, and security mechanisms.;

Security strength requirements associated with such capabilities, functions, and mechanisms shall include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass;

Security assurance requirements;

* 1. Development processes, procedures, practices, and methodologies;
  2. Evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved

1. Security-related documentation requirements;
2. Requirements for protecting security-related documentation;
3. Description of the information system development environment and environment in which the system is intended to operate; and
4. Acceptance criteria.

#### Control Implementation Description:

*<<Description of control implementation>>*

SA-4(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SA-4(1) Acquisition Process – Functional Properties of Security Controls

#### North Carolina / NIST 800-53 Control Objective:

The agency requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

#### Control Implementation Description:

*<<Description of control implementation>>*

SA-4(2) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SA-4(2) Acquisition Process – Design/Implementation Information for Security Controls

#### North Carolina / NIST 800-53 Control Objective:

The agency requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes the following: security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics.

Agencies may require different levels of detail in design and implementation documentation for security controls employed in agency information systems, system components, or information system services based on mission/business requirements, requirements for trustworthiness/resiliency, and requirements for analysis and testing.

#### Control Implementation Description:

*<<Description of control implementation>>*

SA-4(9) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SA-4(9) Acquisition Process – Functions/Ports/Protocols/Services in Use

#### North Carolina / NIST 800-53 Control Objective:

The agency requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SA-5 Information System Documentation

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Obtains administrator documentation for the information system, system component, or information system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service;
   2. Effective use and maintenance of security functions/mechanisms; and
   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
2. Obtains user documentation for the information system, system component, or information system service that describes:
   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
   3. User responsibilities in maintaining the security of the system, component, or service;
3. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and takes [Assignment: organization-defined actions] in response;
4. Protects documentation as required, in accordance with the risk management strategy; and
5. Distributes documentation to [Assignment: organization-defined personnel or roles].

#### Control Implementation Description:

*<<Description of control implementation>>*

SA-8 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SA-8 Security Engineering Principles

#### North Carolina / NIST 800-53 Control Objective:

The agency applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SA-9 External Information System Services

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Requires that providers of external information system services comply with organizational
2. information security requirements and employ a formal service level agreement (SLA) in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
3. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
4. Employs agency-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

#### Control Implementation Description:

*<<Description of control implementation>>*

SA-9(2) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SA-9(2) External Information System Services – Identification of Functions / Ports / Protocols / Services

#### North Carolina / NIST 800-53 Control Objective:

The agency requires providers of external information system services to identify the functions, ports, protocols, and other services required for the use of such services.

#### Control Implementation Description:

*<<Description of control implementation>>*

SA-10 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SA-10 Developer Configuration Management

#### North Carolina / NIST 800-53 Control Objective:

The agency requires the developer of the information system, system component, or information system service to:

1. Perform configuration management during information system design, development, implementation, and operation for the following;
   1. Internal system development and system integration of commercial software
   2. External system development and system integration
2. Document, manage, and control the integrity of changes to the information system or configuration items under configuration management;
3. Implement only agency-approved changes to the system, component, or service;
4. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
5. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].

#### Control Implementation Description:

*<<Description of control implementation>>*

SA-11 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SA-11 Developer Security Testing and Evaluation

#### North Carolina / NIST 800-53 Control Objective:

The agency requires the developer of the information system, system component, or information system service to:

1. Create and implement a security test and evaluation plan;
2. Perform unit, integration, system; regression testing/evaluation:
   1. Require that information system developers/integrators perform a vulnerability assessment to document vulnerabilities, exploitation potential, and risk mitigations.
   2. Vulnerability assessments and penetration tests are tools that can minimize opportunities for cyber- crime and are part of a defense-in-depth strategy. When an agency determines that an assessment of information system security or network vulnerability is needed, it shall receive approval from the State CIO, as required by N.C.G.S. §143B-1377(d).
   3. Appropriate testing and assessment activities shall be performed after vulnerability mitigation plans have been executed to verify and validate that the vulnerabilities have been successfully addressed.
   4. To maintain the integrity of agency information technology systems, software shall be evaluated and certified for functionality in a test environment before it is used in an operational/production environment.
   5. Test data and accounts shall be removed from an application or system prior to being deployed into a production environment if the application or system does not have a dedicated testing environment.
   6. Qualified personnel must certify that the upgrade or change has passed acceptance testing.
   7. A rollback plan must be established in the event the upgrade or change has unacceptable ramifications.
3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
4. Implement a verifiable flaw remediation process; and
5. Correct flaws identified during security testing/evaluation.

#### Control Implementation Description:

*<<Description of control implementation>>*

SA-12 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SA-12 Supply Chain Protection

#### North Carolina / NIST 800-53 Control Objective:

The agency protects against supply chain threats to the information system, system component, or information system service by employing agency-defined security safeguards that include conducting a supplier review prior to entering into a contractual agreement to acquire the information system, system component, or information system service

#### Control Implementation Description:

*<<Description of control implementation>>*

SA-13 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SA-13 Trustworthiness

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Describes the trustworthiness required in the (the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information it processes, stores, or transmits) that are required in information systems, information system components, or information system services supporting its critical missions/business functions; and
2. Implements [Assignment: organization-defined assurance overlay] to achieve such trustworthiness.

#### Control Implementation Description:

*<<Description of control implementation>>*

SA-14 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SA-14 Criticality Analysis

#### North Carolina / NIST 800-53 Control Objective:

The agency identifies critical information system components and functions by performing a criticality analysis for information systems, information system components, or information system services throughout agency-defined decision points in the system development life cycle.

#### Control Implementation Description:

*<<Description of control implementation>>*

SA-15 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SA-15 Development Process, Standards, and Tools

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Requires the developer of the information system, system component, or information system service to follow a documented development process that:
   1. Explicitly addresses security requirements;
   2. Identifies the standards and tools used in the development process;
   3. Documents the specific tool options and tool configurations used in the development process; and
   4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
2. Reviews the development process, standards, tools, and tool options/configurations annually to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy agency-defined security requirements.

#### Control Implementation Description:

*<<Description of control implementation>>*

SA-16 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SA-16 Developer Provided Training

#### North Carolina / NIST 800-53 Control Objective:

The agency requires the developer of the information system, system component, or information system service to provide at least the manager / custodian on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

#### Control Implementation Description:

*<<Description of control implementation>>*

SA-17 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SA-17 Developer Security Architecture and Design

#### North Carolina / NIST 800-53 Control Objective:

The agency requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:

1. Is consistent with and supportive of the organization’s security architecture which is established within and is an integrated part of the organization’s enterprise architecture;
2. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
3. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

#### Control Implementation Description:

*<<Description of control implementation>>*

SA-18 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SA-18 Tamper Resistance and Detection

#### North Carolina / NIST 800-53 Control Objective:

The agency implements a tamper protection program for the information system, system component, or information system service.

#### Control Implementation Description:

*<<Description of control implementation>>*

SA-19 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SA-19 Component Authenticity

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; and
2. Reports counterfeit information system components to law enforcement and the source of counterfeit component;

#### Control Implementation Description:

*<<Description of control implementation>>*

SA-20 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SA-20 Customized Development of Critical Components

#### North Carolina / NIST 800-53 Control Objective:

The agency re-implements or custom develops agency-defined critical information system components.

#### Control Implementation Description:

*<<Description of control implementation>>*

SA-21 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SA-21 Developer Screening

#### North Carolina / NIST 800-53 Control Objective:

The agency requires that the developer information system, system component, or information system service:

1. Have appropriate access authorizations as determined by assigned system manager / custodian; and
2. Satisfy agency personnel screening criteria].

#### Control Implementation Description:

*<<Description of control implementation>>*

SA-22 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SA-22 Unsupported System Component

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and
2. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

#### Control Implementation Description:

*<<Description of control implementation>>*

## System and Communication Protection (SC)

### SC-1 System and Communications Protection Policy and Procedures

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops, documents, and disseminates to all covered personnel involved in the implementation or operation of system and communications protection controls:
   1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and
2. Reviews and updates the current:
   1. System and communications protection policy annually, at a minimum; and
   2. System and communications protection procedures [Assignment: organization-defined frequency].

#### Control Implementation Description:

*<<Description of control implementation>>*

### SC-2 Application Partitioning

#### North Carolina / NIST 800-53 Control Objective:

The information system separates user functionality (including user interface services) from information system management functionality.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-3 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-3 Security Function Isolation

#### North Carolina / NIST 800-53 Control Objective:

The information system isolates security functions from non-security functions.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-4 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-4 Information in Shared Resources

#### North Carolina / NIST 800-53 Control Objective:

The information system prevents unauthorized and unintended information transfer via shared system resources.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SC-5 Denial of Service Protection

#### North Carolina / NIST 800-53 Control Objective:

The information system protects against or limits the effects of denial of service (DOS) attacks by doing the following:

1. Denying all inbound traffic by default, thus limiting the channels of network attacks;
2. Periodically scanning network and devices for bots (software robots) and Trojan horse programs;
3. Deploying authentication mechanisms wherever possible;
4. Designing and implementing networks for maximum resiliency;
5. Developing specific plans for responding to DoS and DDoS attacks in the agency incident management plan and the business continuity plan;
6. Managing excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks;
7. Providing detection and monitoring capabilities to detect indicators of denial of service attacks against the agency and to determine if sufficient resources exist to prevent effective denial of service attacks.
8. Additional guidance is available NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-6 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-6 Resource Availability

#### North Carolina / NIST 800-53 Control Objective:

The information system protects the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more); priority; quota; [Assignment: organization-defined security safeguards]].

#### Control Implementation Description:

*<<Description of control implementation>>*

### SC-7 Boundary Protection

#### North Carolina / NIST 800-53 Control Objective:

Agencies shall do the following:

1. Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with statewide security architecture requirements. Managed interfaces include, for example, gateways, routers, firewalls, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within the security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks).
2. Establish a traffic flow policy for each managed interface.
3. Protect the confidentiality and integrity of the information being transmitted across each interface.
4. Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need.
5. Review exceptions to the traffic flow policy annually and remove exceptions that are no longer supported by an explicit mission/business need.
6. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system
7. Implement subnetworks for publicly accessible system components that are physically and logically separated from internal agency network.
8. Agencies shall limit the number of external network connections to the information system. Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic.
9. Protective controls shall at a minimum include the following:
   1. Positive source and destination address checking to restrict rogue networks from manipulating the State’s routing tables;
   2. Firewalls must use an authentication mechanism that provides accountability for the individual and to ensure device configuration does not become corrupted with false entries;
   3. Screen internal network addresses from external view;
   4. Information systems at managed interfaces shall deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.
10. Network routing controls should be implemented to supplement equipment identification by allowing specific equipment to connect only from specified external networks or internal sub networks (“subnets”).
11. Web applications should be developed to use a minimum number of ports to allow for easy integration in traditional demilitarized zone (DMZ—filtered subnet) environments.
12. Firewalls shall be configured to the following specifications:
    1. Local user accounts shall be configured on network firewalls, for the sole purpose of eliminating possible extended outages.
    2. Local accounts shall be configured to only become active when the device cannot make contact with the central unit. During normal operation, the local account exists, but is unusable.
    3. Passwords on firewalls shall be kept in a secure encrypted form as required by the Identification and Authentication Policy SCIO-SEC-307, Section IA-5 Authenticator Management.
    4. All agencies shall designate a minimum of two (2) authorized firewall administrators. At least one of the designated firewall administrators will be a security specialist who is consulted before firewall policy changes are approved and implemented.
    5. For temporary or emergency port openings, the agency process shall establish a maximum time for the port to be open, which shall not exceed 5 days. The agency authorized firewall policy administrators, or the entity managing the firewall, shall subsequently close the port or develop additional hardening.
    6. System administrators shall configure the firewall so that it cannot be identifiable as such to other network(s), or, at most, appears to be just another router.
    7. Firewalls shall be installed in locations that are physically secure from tampering. The agency security liaison shall approve the physical location of the firewalls. Firewalls shall not be relocated without the prior approval of the agency security liaison.
    8. Firewall rules sets shall always block the following types of network traffic:
       1. Web requests that are not from an authorized internal web proxy must not be passed to the Internet
       2. Information systems must detect and block unauthorized scanning activity that originates outside of its network, within its network, and between information systems.
       3. Inbound network traffic from a non-authenticated source system with a destination address of the firewall system itself;
       4. Inbound network traffic with a source address indicating that the packet originated on a network behind the firewall;
       5. Traffic inbound to the State Network containing ICMP (Internet Control Message Protocol) traffic will be blocked at the perimeter with the following exceptions: To allow testing initiated from internal IT support groups, ICMP echo replies and ICMP TTL expired will be permitted inbound to the State Network but will be limited to specific IP addresses or small subnets representing the internal support group. A ping point can be established at the perimeter, for troubleshooting purposes, with the sole purpose and sole capability of responding to a ping;
       6. Inbound network traffic containing IP Source Routing information;
       7. Inbound or outbound network traffic containing a source or destination address of 0.0.0.0 and/or containing directed broadcast addresses.
    9. Logging features on State Network firewalls shall capture all packets dropped or denied by the firewall, and agency staff or the entity managing the firewall shall review those logs at least monthly.
    10. Each agency’s firewall policy shall be reviewed and verified by agency 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 agency’s firewall policy at least quarterly.
    11. Additional requirements for protecting federal tax information (FTI) on networks are provided in Section 9.4.10, Network Protections.
    12. Firewall configurations and associated documentation must be treated as restricted information and must be available to only authorized personnel (e.g., authorized administrators, auditors, security oversight personnel).
13. Information systems, in conjunction with a remote device, shall prevent the device from simultaneously establishing non-remote connections (i.e. split tunneling) with the system and communicating via some other connection to resources in external networks.
14. NIST SP 800-41, Revision 1 must be used as guidance on firewalls and firewall policy.
15. NIST SP 800-54 must be used as guidance on routers.
16. NIST SP 800-77 must be used as guidance on Virtual Private Networks (VPNs).
17. NIST SP 800-94 must be used as guidance on IDPS.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SC-8 Transmission Confidentiality and Integrity

#### North Carolina / NIST 800-53 Control Objective:

Agencies shall protect confidentiality and integrity of transmitted information to ensure that the confidentiality and integrity of the data are maintained during the transfer process.

1. Agencies shall implement safeguards to protect network cabling from being damaged and to reduce the possibility of unauthorized interception of data transmissions that take place across such cabling. (NC Electrical Code, Chapter 8, Article 830) The agency must ensure that all network infrastructure, access points, wiring, conduits, and cabling are within the control of authorized agency personnel.
2. Network monitoring capabilities must be implemented to detect and monitor for suspicious network traffic.
3. Agencies shall deploy controls to ensure that the State’s resources do not contribute to outside-party attacks. These controls include the following:
   1. Securing interfaces between agency-controlled and non-agency-controlled or public networks
   2. Standardizing authentication mechanisms in place for both users and equipment
   3. Controlling users’ access to information resources
   4. Monitoring for anomalies or known signatures via intrusion detection systems (IDS) and/or intrusion prevention systems (IPS). IDPS signatures shall be up to date
4. Public employees and other State Network users shall not intercept or attempt to intercept data transmissions of any kind that they are not authorized to access.
5. Each agency shall document and retain on file a case-by-case risk management determination for each type of confidential information as to the appropriateness of its unencrypted transmission to a party not served by the agency’s internal network
6. Agencies shall address the risk involved in the transfer of different types of data and implement safeguards through the means of exchange used, such as through email, the Internet, or exchange of electronic media and tapes.
7. Agencies should implement formal procedures that require both the sender of the information and the intended recipient to authorize the facsimile transmission and recipient facsimile phone number before the transmission occurs and to verify successful transmission upon receipt.
8. Agencies shall use secure protocols, such as Secure Shell (SSH), Transport Layer Security (TLS), and Internet Protocol Security (IPSec), for secure network management functions.
9. All communications that transfer confidentially sensitive data between web clients and web servers must employ the most current secure transport protocol that includes the most recent version of Transport Layer Security (TLS).
10. NIST SP 800-52 must be used as guidance on protecting transmission integrity using TLS.
11. NIST SP 800-77 must be used as guidance on protecting transmission integrity using IPsec.
12. NIST SP 800-81 must be used as guidance on Domain Name System (DNS) message authentication and integrity verification.
13. NIST SP 800-113 must be used as guidance on SSL VPNs.
14. Instant messaging technologies, where allowed, must not be used to transmit any type of Restricted or highly Restricted data.
15. The following types of transmission require enhanced protection (e.g., cryptography mechanisms) when integrity is an important consideration:
    1. Internal traffic within the information system and applications
    2. Internal traffic between two or more information systems
    3. External traffic to or across the Internet
    4. Remote access
    5. Email
    6. FTP transmissions
    7. Web services
    8. Voice over Internet Protocol (VoIP)
    9. Audio and video
    10. Wireless client to host communications
16. Agencies shall implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or to detect changes to information during transmission unless otherwise protected by alternative physical safeguards.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SC-10 Network Disconnect

#### North Carolina / NIST 800-53 Control Objective:

The information system terminates the network connection associated with a communications session at the end of the session or after 30 minutes of inactivity.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-11 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-11 Trusted Path

#### North Carolina / NIST 800-53 Control Objective:

The information system establishes a trusted communications path between the user and the following security functions of the system: [Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication].

#### Control Implementation Description:

*<<Description of control implementation>>*

### SC-12 Cryptographic Key Establishment and Management

#### North Carolina / NIST 800-53 Control Objective:

The agency establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with agency-defined requirements for key generation, distribution, storage, access, and destruction.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SC-13 Cryptographic Protection

#### North Carolina / NIST 800-53 Control Objective:

The information system implements cryptographic modules in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SC-15 Collaborative Computing Devices

#### North Carolina / NIST 800-53 Control Objective:

The information system:

1. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and
2. Provides an explicit indication of use to users physically present at the devices.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-16 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-16 Transmission of Security Attributes

#### North Carolina / NIST 800-53 Control Objective:

The information system associates [Assignment: organization-defined security attributes] with information exchanged between information systems and between system components.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SC-17 Public Key Infrastructure Certificates

#### North Carolina / NIST 800-53 Control Objective:

The agency issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates from an approved service provider.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SC-18 Mobile Code

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Defines acceptable and unacceptable mobile code and mobile code technologies;
2. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
3. Authorizes, monitors, and controls the use of mobile code within the information system.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SC-19 Voice Over Internet Protocol

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
2. Authorizes, monitors, and controls the use of VoIP within the information system.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SC-20 Secure Name /Address Resolution Service (Authoritative Source)

#### North Carolina / NIST 800-53 Control Objective:

The information system:

1. Provides additional data origin authentication and integrity verification artifacts along with the
2. authoritative name resolution data the system returns in response to external name/address resolution queries; and
3. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SC-21 Secure Name /Address Resolution Service (Recursive or Caching Resolver)

#### North Carolina / NIST 800-53 Control Objective:

The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SC-22 Architecture and Provisioning for Name/Address Resolution Service

#### North Carolina / NIST 800-53 Control Objective:

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SC-23 Session Authenticity

#### North Carolina / NIST 800-53 Control Objective:

The information system protects the authenticity of communications sessions.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-24 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-24 Fail in Known State

#### North Carolina / NIST 800-53 Control Objective:

The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-25 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-25 Thin Nodes

#### North Carolina / NIST 800-53 Control Objective:

The agency employs [Assignment: organization-defined information system components] with minimal functionality and information storage.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-26 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-26 Honeypots

#### North Carolina / NIST 800-53 Control Objective:

The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-27 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-27 Platform-Independent Applications

#### North Carolina / NIST 800-53 Control Objective:

The information system includes: [Assignment: organization-defined platform-independent applications].

#### Control Implementation Description:

*<<Description of control implementation>>*

### SC-28 Protection of Information at Rest

#### North Carolina / NIST 800-53 Control Objective:

The information system protects the confidentiality and integrity of all restricted or highly restricted data at rest.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-29 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-29 Heterogeneity

#### North Carolina / NIST 800-53 Control Objective:

The agency employs a diverse set of information technologies for [Assignment: organization-defined information system components] in the implementation of the information system.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-30 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-30 Concealment and Misdirection

#### North Carolina / NIST 800-53 Control Objective:

The agency employs [Assignment: organization-defined concealment and misdirection techniques] for [Assignment: organization-defined information systems] at [Assignment: organization-defined time periods] to confuse and mislead adversaries.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-31 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-31 Covert Channel Analysis

#### North Carolina / NIST 800-53 Control Objective:

The organization:

1. Performs a covert channel analysis to identify those aspects of communications within the information system that are potential avenues for covert [Selection (one or more): storage; timing] channels; and
2. Estimates the maximum bandwidth of those channels.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-32 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-32 Information System Partitioning

#### North Carolina / NIST 800-53 Control Objective:

The agency partitions the information system into [Assignment: organization-defined information system components] residing in separate physical domains or environments based on [Assignment: organization-defined circumstances for physical separation of components].

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-34 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-34 Non-Modifiable Executable Programs

#### North Carolina / NIST 800-53 Control Objective:

The information system at [Assignment: organization-defined information system components]:

1. Loads and executes the operating environment from hardware-enforced, read-only media; and
2. Loads and executes [Assignment: organization-defined applications] from hardware-enforced, read-only media.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-35 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-35 Honeyclients

#### North Carolina / NIST 800-53 Control Objective:

The information system includes components that proactively seek to identify malicious websites and/or web-based malicious code.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-36 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-36 Distributed Processing and Storage

#### North Carolina / NIST 800-53 Control Objective:

The agency distributes [Assignment: organization-defined processing and storage] across multiple physical locations.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-37 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-37 Out-of-Band Channels

#### North Carolina / NIST 800-53 Control Objective:

The agency employs [Assignment: organization-defined out-of-band channels] for the physical delivery or electronic transmission of [Assignment: organization-defined information, information system components, or devices] to [Assignment: organization-defined individuals or information systems].

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-38 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-38 Operations Security

#### North Carolina / NIST 800-53 Control Objective:

The agency employs [Assignment: organization-defined operations security safeguards] to protect key organizational information throughout the system development life cycle.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-39 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-39 Process Isolation

#### North Carolina / NIST 800-53 Control Objective:

The information system maintains a separate execution domain for each executing process.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SC-40 Wireless Link Protection

#### North Carolina / NIST 800-53 Control Objective:

The information system protects external and internal wireless links from corruption or data loss.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-41 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-41 Port and I/O Device Access

#### North Carolina / NIST 800-53 Control Objective:

The agency physically disables or removes [Assignment: organization-defined connection ports or input/output devices] on [Assignment: organization-defined information systems or information system components].

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-42 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-42 Sensor Capability and Data

#### North Carolina / NIST 800-53 Control Objective:

The information system:

1. Prohibits the remote activation of environmental sensing capabilities with the following exceptions: [Assignment: organization-defined exceptions where remote activation of sensors is allowed]; and
2. Provides an explicit indication of sensor use to [Assignment: organization-defined class of users].

#### Control Implementation Description:

*<<Description of control implementation>>*

### SC-43 Usage Restrictions

#### North Carolina / NIST 800-53 Control Objective:

The agency:

a. Establishes usage restrictions and implementation guidance for information system components based on the potential to cause damage to the information system if used maliciously; and

b. Authorizes, monitors, and controls the use of such components within the information system.

#### Control Implementation Description:

*<<Description of control implementation>>*

SC-44 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SC-44 Detonation Chambers

#### North Carolina / NIST 800-53 Control Objective:

Agencies should employ a detonation chamber capability also known as dynamic execution environments to do the following:

1. Allow the opening of email attachments.
2. Allow the execution of untrusted or suspicious applications.
3. Allow the execution of Universal Resource Locator (URL) requests in the safety of an isolated environment or virtualized sandbox to quickly identify malicious code.
4. Reduce the likelihood that the code is propagated to user environments of operation (or prevent such propagation completely).
5. This control is optional for LOW risk information systems.

#### Control Implementation Description:

*<<Description of control implementation>>*

## System and Information Integrity (SI)

### SI-1 System and Information Integrity Policy and Procedures

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Develops, documents, and disseminates to all covered personnel involved in the deployment, operation and maintenance of information systems and supporting infrastructure:
   1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
2. Reviews and updates the current:
   1. System and information integrity policy reviewed; and
   2. System and information integrity procedures [Assignment: organization-defined frequency].

#### Control Implementation Description:

*<<Description of control implementation>>*

### SI-2 Flaw Remediation

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Identifies, reports, and corrects information system flaws;
2. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
3. Based on risk, agency installs security-relevant software and firmware updates within the following agency-defined time periods
   1. **Critical-level risk** vulnerabilities must be mitigated as soon as possible. “Critical-level risk” vulnerabilities must be, at a minimum, mitigated within seven (7) days, and remediated (if possible) within twenty-one (21) days.
   2. **High-level risk** vulnerabilities must be mitigated or remediated within thirty (30) days.
   3. **Medium-level risk** vulnerabilities must be mitigated or remediated within sixty (60) days.
   4. **Low-level risk** vulnerabilities must be mitigated or remediated within ninety (90) days.; and
4. Incorporates flaw remediation into the organizational configuration management process.

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-2(2) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-2(2) Flaw Remediation | Automated Flaw Remediation Status

#### North Carolina / NIST 800-53 Control Objective:

The agency employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SI-3 Malicious Code Protection

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
2. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
3. Configures malicious code protection mechanisms to:
   1. Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at system entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and
   2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and
4. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-3(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-3(1) Malicious Code Protection | Central Management

#### North Carolina / NIST 800-53 Control Objective:

The agency centrally manages malicious code protection mechanisms.

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-3(2) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-3(2) Malicious Code Protection | Automatic Updates

#### North Carolina / NIST 800-53 Control Objective:

The information system automatically updates malicious code protection mechanisms.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SI-4 Information System Monitoring

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Monitors the information system to detect:
   1. Attacks and indicators of potential attacks in accordance with agency-defined monitoring objectives; and
   2. Unauthorized local, network, and remote connections;
2. Identifies unauthorized use of the information system through State / agency-defined management and monitoring standards];
3. Deploys monitoring devices:
   1. Strategically within the information system to collect organization-determined essential information; and
   2. At ad hoc locations within the system to track specific types of transactions of interest to the agency;
4. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
5. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
6. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
7. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-4(2) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-4(2) Information System Monitoring | Automated Tools for Real-Time Analysis

#### North Carolina / NIST 800-53 Control Objective:

The agency employs automated tools to support near real-time analysis of events.

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-4(4) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-4(4) Information System Monitoring | Inbound And Outbound Communications Traffic

#### North Carolina / NIST 800-53 Control Objective:

The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions.

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-4(5) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-4(5) Information System Monitoring | System-Generated Alerts

#### North Carolina / NIST 800-53 Control Objective:

The information system authorized personnel when the following indications of compromise or potential compromise occur: audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SI-5 Security Alerts, Advisories, and Directives

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Receives information system security alerts, advisories, and directives from external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations on an ongoing basis;
2. Generates internal security alerts, advisories, and directives as deemed necessary;
3. Disseminates security alerts, advisories, and directives to: agency management and technical staff as appropriate; and
4. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-6 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-6 Security Function Verification

#### North Carolina / NIST 800-53 Control Objective:

The information system:

1. Verifies the correct operation of the following security function:
   1. User login activity, both failed and successful, including user IDs, log-in date/time, log-out date/time.
   2. Unauthorized access attempts to network or system resources, including audit files.
   3. Changes to critical application system files.
   4. Changes to system security parameters.
   5. System start-ups and shut-downs.
   6. Application start up, restart and/or shutdown.
   7. Attempts to initialize, remove, enable or disable accounts or services.
   8. Changes to the auditing function, including enabling or disabling auditing and changing events to be audited.
   9. User credential creation and deletion.
   10. Attempts to create, remove or set passwords or change system privileges.
   11. All uses of special system privileges.
   12. System errors and corrective action(s) taken.
   13. Failed read-and-write operations on the system directory.
   14. All actions taken with administrative privileges.
2. Performs this verification [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]];
3. Notifies [Assignment: organization-defined personnel or roles] of failed security verification tests; and
4. [Selection (one or more): shuts the information system down; restarts the information system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-7 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-7 Software, Firmware, and Information Integrity

#### North Carolina / NIST 800-53 Control Objective:

The agency employs integrity verification tools to detect unauthorized changes to agency software, firmware, and information].

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-7(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-7(1) Software, Firmware, and Information Integrity | Integrity Checks

#### North Carolina / NIST 800-53 Control Objective:

The information system performs an integrity check of agency-defined software, firmware, and information at transitional states, such as, system startup, restart, shutdown, and abort, as well as when any security-relevant events occur

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-7(7) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-7(7) Software, Firmware, and Information Integrity | Integrity of Detection And Response

#### North Carolina / NIST 800-53 Control Objective:

The agency incorporates the detection of unauthorized security-relevant changes to the information system into the organizational incident response capability.

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-8 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-8 Spam Protection

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
2. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-8(1) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-8(1) Spam Protection | Central Management

#### North Carolina / NIST 800-53 Control Objective:

The agency centrally manages spam protection mechanisms.

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-8(2) Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-8(2) Spam Protection | Automatic Updates

#### North Carolina / NIST 800-53 Control Objective:

The information system automatically updates spam protection mechanisms.

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-10 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-10 Information Input Validation

#### North Carolina / NIST 800-53 Control Objective:

The information system checks the validity of information inputs.

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-11 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-11 Error Handling

#### North Carolina / NIST 800-53 Control Objective:

The information system:

1. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
2. Reveals error messages only to designated agency personnel.

#### Control Implementation Description:

*<<Description of control implementation>>*

### SI-12 Information Handling and Retention

#### North Carolina / NIST 800-53 Control Objective:

The agency handles and retains information within the information system and information output from the system in accordance with applicable federal laws, directives, policies, regulations, State standards, and operational requirements.

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-13 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-13 Predictable Failure Prevention

#### North Carolina / NIST 800-53 Control Objective:

The agency:

1. Determines mean time to failure (MTTF) for non-repairable security system components in production and backup environments of operation; and
2. Provides substitute information system components and a means to exchange active and standby components at agency-defined MTTF value with consideration for resulting potential hard from component failure.

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-14 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-14 Non-Persistence

#### North Carolina / NIST 800-53 Control Objective:

The agency implements non-persistent information system components and services that are initiated in a known state and terminated upon end of session of use.

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-15 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-15 Information Output Filtering

#### North Carolina / NIST 800-53 Control Objective:

The information system validates information output from agency-defined software programs and/or applications to ensure that the information is consistent with the expected content.

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-16 Control Notes:

NC DIT has identified this control as MANDATORY for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

For a Moderate system update the control entry to document the control implementation as with any other control.

If choosing to implement this optional control for a Low sensitivity system, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control for a Low sensitivity system, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-16 Memory Protection

#### North Carolina / NIST 800-53 Control Objective:

The information system implements security safeguards to protect its memory from unauthorized code execution.

#### Control Implementation Description:

*<<Description of control implementation>>*

SI-17 Control Notes:

NC DIT has identified this control as OPTIONAL for Moderate sensitivity information systems.

NC DIT has identified this control as OPTIONAL for Low sensitivity information systems.

If choosing to implement this optional control, update the control entry to document the control implementation as with any other control.

If choosing not to implement this optional control, either delete the entire control entry or update the control entry to document the decision.

Delete this note box after deleting or updating the control entry.

### SI-17 Fail-Safe Procedures

#### North Carolina / NIST 800-53 Control Objective:

The information system implements fail-safe procedures when agency-defined failure conditions occur.

#### Control Implementation Description:

*<<Description of control implementation>>*

1. Classification of systems in terms of security impact is further defined in Appendix III to OMB Circular No. A-130 - Security of Federal Automated Information Resources [↑](#footnote-ref-1)