North Carolina Department of Information Technology

Statewide Information Security Manual

January 2018
INTRODUCTION

PURPOSE

The purpose of this policy is to establish a statewide security policy for North Carolina State agencies and the State network. This policy also establishes principles to ensure a secure network infrastructure that integrates confidentiality, availability, and integrity into the infrastructure design, implementation, and maintenance, in order to do the following:

a. Protect the State’s infrastructure and the citizen’s data, whether hosted by external entities or within State data centers, from both internal and external threats.

b. Provide a consistent and repeatable framework for which IT assets can be securely connected to the State network.

c. Support the State’s initiative to establish standards to manage technology, risks and increase consistency and accessibility.

OWNER
State Chief Risk Officer

SCOPE

The Statewide Information Security Manual is the foundation for information technology security in North Carolina. It sets out the statewide information security standards required by N.C.G.S. §143B-1376, which directs the State Chief Information Officer (State CIO) to establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the State’s distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. These standards apply to all executive branch agencies, their agents or designees subject to Article 15 of N.C.G.S. §143B. Use by local governments, local education agencies (LEAs), community colleges, constituent institutions of the University of North Carolina (UNC) and other executive branch agencies is encouraged to the extent allowed by law.

POLICY

SECTION 1. ADOPTION OF NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) RISK MANAGEMENT FRAMEWORK SPECIAL PUBLICATION (SP) 800-37

The State has adopted the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 – Guide for Applying Risk Management Framework (RMF) for Federal Information Systems, as the standard for managing information security risk in State IT resources. The RMF provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. The NIST RMF utilizes NIST SP 800-53 as the foundation for identifying and implementing security controls. NIST 800-53 Rev 4 organizes these security controls into (17) Control Families. Table 1 identifies the control family names which will be utilized within the State security policies.

TABLE 1: SECURITY CONTROL FAMILY NAMES
There are two levels of security categorization to be used within the State: **Low** and **Moderate**. Security controls must be selected based on the data classification and security categorization of the information system and/or requirements for the specific operating environment.

**Low Systems**: Systems that contain only data that is public by law or directly available to the public via such mechanisms as the Internet. In addition, desktops, laptops and supporting systems used by agencies are Low Risk unless they store, process, transfer or communicate Restricted or Highly Restricted data.

**Moderate Systems**: Systems that stores, process, transfer or communicate Restricted or Highly Restricted data or has a direct dependency on a Moderate system. Any system that stores, processes, or transfers or communicates PII or other sensitive data types is classified as a Moderate system, at a minimum.

Agencies may tailor the baseline controls, as needed to enhance the security posture, based on their unique organizational needs. An example of such enhancement may occur due to additional requirements mandated by Federal agencies such as Internal Revenue Service (IRS) and other. All agencies are required to implement and comply with the baseline controls within the Statewide Information Security Manual, unless otherwise prescribed by Federal or State statute.

NIST SP 800-53 controls defines three types of controls:

- **Common Controls**: Those security controls that are Enterprise wide, e.g. State policies, Security devices provided by DIT, Enterprise email, etc. Agencies may inherit these controls as the system is managed outside of their authority. It is important to note that in order for a system to be considered Inherited, it must meet, at a minimum, the following criteria:
  - The system is managed by DIT, Cloud or other organizations outside the authority and security boundary of the agency
  - The State Chief Risk Officer has designated the control as inheritable

- **System-Specific Controls**: Those controls that provide security and other services for a particular information system only

- **Hybrid Controls**: Those controls which are shared between Enterprise, i.e. DIT, Cloud and/or Agency managed.

Agencies must evaluate each system and identify those that fall within the above listed control types. This step is crucial in facilitating and understanding roles and responsibilities as it pertains to audits and assessments. The following Table 2 - **Security Control Baseline** identifies those controls that will be implemented if a system is
categorized as Low or Moderate. The table is based on NIST 800-53 Rev 4 and has been modified to meet State of North Carolina use.

**Note:** Optional controls which have brackets, e.g. (X) are enhanced controls above the baseline requirement. Controls listed as “Optional” may be utilized to enhance the security posture of the information system. These controls are NOT to be considered mandatory. Agencies should understand that with the implementation of these controls may require additional funding. The description of these controls may be found at the following link: https://web.nvd.nist.gov/view/800-53/Rev4/home.

### TABLE 2: SECURITY CONTROL BASELINES

<table>
<thead>
<tr>
<th>CNTL NO.</th>
<th>CONTROL NAME</th>
<th>INITIAL CONTROL BASELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>ACCESS CONTROL</strong></td>
<td></td>
</tr>
<tr>
<td>AC-1</td>
<td>Access Control Policy and Procedures</td>
<td>AC-1</td>
</tr>
<tr>
<td>AC-2</td>
<td>Account Management</td>
<td>AC-2</td>
</tr>
<tr>
<td>AC-3</td>
<td>Access Enforcement</td>
<td>AC-3</td>
</tr>
<tr>
<td>AC-4</td>
<td>Information Flow Enforcement</td>
<td>AC-4 (1) (2) (3) (4)</td>
</tr>
<tr>
<td>AC-5</td>
<td>Separation of Duties</td>
<td>AC-5</td>
</tr>
<tr>
<td>AC-6</td>
<td>Least Privilege</td>
<td>AC-6</td>
</tr>
<tr>
<td>AC-7</td>
<td>Unsuccessful Logon Attempts</td>
<td>AC-7</td>
</tr>
<tr>
<td>AC-8</td>
<td>System Use Notification</td>
<td>AC-8</td>
</tr>
<tr>
<td>AC-9</td>
<td>Previous Logon (Access) Notification</td>
<td>Optional</td>
</tr>
<tr>
<td>AC-10</td>
<td>Concurrent Session Control</td>
<td>Optional</td>
</tr>
<tr>
<td>AC-11</td>
<td>Session Lock</td>
<td>AC-11 (1)</td>
</tr>
<tr>
<td>AC-12</td>
<td>Session Termination</td>
<td>AC-12</td>
</tr>
<tr>
<td>AC-14</td>
<td>Permitted Actions without Identification or Authentication</td>
<td>AC-14</td>
</tr>
<tr>
<td>AC-16</td>
<td>Security Attributes</td>
<td>Optional</td>
</tr>
<tr>
<td>AC-17</td>
<td>Remote Access</td>
<td>AC-17 (1) (2) (3) (4)</td>
</tr>
<tr>
<td>AC-18</td>
<td>Wireless Access</td>
<td>AC-18</td>
</tr>
<tr>
<td>AC-19</td>
<td>Access Control for Mobile Devices</td>
<td>AC-19 (5)</td>
</tr>
<tr>
<td>AC-20</td>
<td>Use of External Information Systems</td>
<td>AC-20 (1) (2)</td>
</tr>
<tr>
<td>AC-21</td>
<td>Information Sharing</td>
<td>AC-21</td>
</tr>
<tr>
<td>AC-22</td>
<td>Publicly Accessible Content</td>
<td>AC-22</td>
</tr>
<tr>
<td>AC-23</td>
<td>Data Mining Protection</td>
<td>Optional</td>
</tr>
<tr>
<td>AC-24</td>
<td>Access Control Decisions</td>
<td>Optional</td>
</tr>
<tr>
<td>AC-25</td>
<td>Reference Monitor</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td><strong>AWARENESS AND TRAINING</strong></td>
<td></td>
</tr>
<tr>
<td>AT-1</td>
<td>Security Awareness and Training Policy and Procedures</td>
<td>AT-1</td>
</tr>
<tr>
<td>AT-2</td>
<td>Security Awareness Training</td>
<td>AT-2</td>
</tr>
<tr>
<td>AT-3</td>
<td>Role-Based Security Training</td>
<td>AT-3</td>
</tr>
<tr>
<td>AT-4</td>
<td>Security Training Records</td>
<td>AT-4</td>
</tr>
<tr>
<td></td>
<td><strong>AUDIT AND ACCOUNTABILITY</strong></td>
<td></td>
</tr>
<tr>
<td>AU-1</td>
<td>Audit and Accountability Policy and Procedures</td>
<td>AU-1</td>
</tr>
<tr>
<td>CNTL NO.</td>
<td>CONTROL NAME</td>
<td>INITIAL CONTROL BASELINES</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td></td>
<td><strong>CONTROL NAME</strong></td>
<td><strong>LOW</strong></td>
</tr>
<tr>
<td>AU-2</td>
<td>Audit Events</td>
<td>AU-2</td>
</tr>
<tr>
<td>AU-3</td>
<td>Content of Audit Records</td>
<td>AU-3</td>
</tr>
<tr>
<td>AU-4</td>
<td>Audit Storage Capacity</td>
<td>AU-4</td>
</tr>
<tr>
<td>AU-5</td>
<td>Response to Audit Processing Failures</td>
<td>AU-5</td>
</tr>
<tr>
<td>AU-6</td>
<td>Audit Review, Analysis, and Reporting</td>
<td>AU-6</td>
</tr>
<tr>
<td>AU-7</td>
<td>Audit Reduction and Report Generation</td>
<td>Optional</td>
</tr>
<tr>
<td>AU-8</td>
<td>Time Stamps</td>
<td>AU-8</td>
</tr>
<tr>
<td>AU-9</td>
<td>Protection of Audit Information</td>
<td>AU-9</td>
</tr>
<tr>
<td>AU-10</td>
<td>Non-repudiation</td>
<td>Optional</td>
</tr>
<tr>
<td>AU-11</td>
<td>Audit Record Retention</td>
<td>AU-11</td>
</tr>
<tr>
<td>AU-12</td>
<td>Audit Generation</td>
<td>AU-12</td>
</tr>
<tr>
<td>AU-13</td>
<td>Monitoring for Information Disclosure</td>
<td>Optional</td>
</tr>
<tr>
<td>AU-14</td>
<td>Session Audit</td>
<td>Optional</td>
</tr>
<tr>
<td>AU-15</td>
<td>Alternate Audit Capability</td>
<td>Optional</td>
</tr>
<tr>
<td>AU-16</td>
<td>Cross-Organizational Auditing</td>
<td>Optional</td>
</tr>
</tbody>
</table>

**Security Assessment and Authorization**

| CA-1    | Security Assessment and Authorization Policies and Procedures | CA-1                      | CA-1                      |
| CA-2    | Security Assessments                                     | CA-2                      | CA-2 (1)                  |
| CA-3    | System Interconnections                                   | CA-3                      | CA-3 (5)                  |
| CA-4    | Security Certification                                    | Incorporated into CA-2.  | Incorporated into CA-2   |
| CA-5    | Plan of Action and Milestones                            | CA-5                      | CA-5                      |
| CA-6    | Security Authorization                                    | CA-6                      | CA-6                      |
| CA-7    | Continuous Monitoring                                     | CA-7                      | CA-7 (1)                  |
| CA-8    | Penetration Testing                                       | Optional                  | Optional                  |
| CA-9    | Internal System Connections                              | CA-9                      | CA-9                      |

**Configuration Management**

| CM-1    | Configuration Management Policy and Procedures          | CM-1                      | CM-1                      |
| CM-2    | Baseline Configuration                                   | CM-2                      | CM-2 (1) (3) (7)          |
| CM-3    | Configuration Change Control                             | CM-3                      | CM-3                      |
| CM-4    | Security Impact Analysis                                  | CM-4                      | CM-4                      |
| CM-5    | Access Restrictions for Change                           | CM-5                      | CM-5                      |
| CM-6    | Configuration Settings                                    | CM-6                      | CM-6                      |
| CM-7    | Least Functionality                                       | CM-7                      | CM-7                      |
| CM-8    | Information System Component Inventory                   | CM-8                      | CM-8 (3)                  |
| CM-9    | Configuration Management Plan                            | CM-9                      | CM-9                      |
| CM-10   | Software Usage Restrictions                              | CM-10                     | CM-10                     |
| CM-11   | User-Installed Software                                  | CM-11                     | CM-11                     |

**Contingency Planning**

<p>| CP-1    | Contingency Planning Policy and Procedures               | CP-1                      | CP-1                      |
| CP-2    | Contingency Plan                                         | CP-2                      | CP-2                      |
| CP-3    | Contingency Training                                     | CP-3                      | CP-3                      |</p>
<table>
<thead>
<tr>
<th>CNTL NO.</th>
<th>CONTROL NAME</th>
<th>INITIAL CONTROL BASELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>LOW</td>
</tr>
<tr>
<td>CP-4</td>
<td>Contingency Plan Testing</td>
<td>CP-4</td>
</tr>
<tr>
<td>CP-5</td>
<td>Contingency Plan Update</td>
<td>Incorporated into CP-2</td>
</tr>
<tr>
<td>CP-6</td>
<td>Alternate Storage Site</td>
<td>Optional</td>
</tr>
<tr>
<td>CP-7</td>
<td>Alternate Processing Site</td>
<td>Optional</td>
</tr>
<tr>
<td>CP-8</td>
<td>Telecommunications Services</td>
<td>Optional</td>
</tr>
<tr>
<td>CP-9</td>
<td>Information System Backup</td>
<td>CP-9</td>
</tr>
<tr>
<td>CP-10</td>
<td>Information System Recovery and Reconstitution</td>
<td>CP-10</td>
</tr>
<tr>
<td>CP-11</td>
<td>Alternate Communications Protocols</td>
<td>Optional</td>
</tr>
<tr>
<td>CP-12</td>
<td>Safe Mode</td>
<td>Optional</td>
</tr>
<tr>
<td>CP-13</td>
<td>Alternative Security Mechanisms</td>
<td>Optional</td>
</tr>
</tbody>
</table>

**Identification and Authentication**

| IA-1 | Identification and Authentication Policy and Procedures | IA-1 | IA-1 |
| IA-2 | Identification and Authentication (Organizational Users) | IA-2 (8) |
| IA-3 | Device Identification and Authentication               | IA-3 | IA-3 |
| IA-4 | Identifier Management                                 | IA-4 | IA-4 |
| IA-5 | Authenticator Management                              | IA-5 | IA-5 |
| IA-6 | Authenticator Feedback                                | IA-6 | IA-6 |
| IA-7 | Cryptographic Module Authentication                    | IA-7 | IA-7 |
| IA-8 | Identification and Authentication (Non-Organizational Users) | IA-8 |
| IA-9 | Service Identification and Authentication              | Optional | Optional |
| IA-10| Adaptive Identification and Authentication             | Optional | Optional |
| IA-11| Re-authentication                                    | Optional | Optional |

**Incident Response**

| IR-1  | Incident Response Policy and Procedures             | IR-1 | IR-1 |
| IR-2  | Incident Response Training                         | IR-2 | IR-2 |
| IR-3  | Incident Response Testing                          | Optional | IR-3 (2) |
| IR-4  | Incident Handling                                  | IR-4 | IR-4 |
| IR-5  | Incident Monitoring                                | IR-5 | IR-5 |
| IR-6  | Incident Reporting                                 | IR-6 | IR-6 |
| IR-7  | Incident Response Assistance                        | IR-7 | IR-7 |
| IR-8  | Incident Response Plan                              | IR-8 | IR-8 |
| IR-9  | Information Spillage Response                       | Optional | Optional |
| IR-10 | Integrated Information Security Analysis Team       | Optional | Optional |

**Maintenance**

<p>| MA-1  | System Maintenance Policy and Procedures            | MA-1 | MA-1 |
| MA-2  | Controlled Maintenance                              | MA-2 | MA-2 |
| MA-3  | Maintenance Tools                                   | Optional | MA-3 (1) (2) |
| MA-4  | Nonlocal Maintenance                                | MA-4 (2) |
| MA-5  | Maintenance Personnel                               | MA-5 | MA-5 |</p>
<table>
<thead>
<tr>
<th>CNTL NO.</th>
<th>CONTROL NAME</th>
<th>INITIAL CONTROL BASELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>LOW</td>
</tr>
<tr>
<td>MA-6</td>
<td>Timely Maintenance</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td><strong>Media Protection</strong></td>
<td></td>
</tr>
<tr>
<td>MP-1</td>
<td>Media Protection Policy and Procedures</td>
<td>MP-1</td>
</tr>
<tr>
<td>MP-2</td>
<td>Media Access</td>
<td>MP-2</td>
</tr>
<tr>
<td>MP-3</td>
<td>Media Marking</td>
<td>Optional</td>
</tr>
<tr>
<td>MP-4</td>
<td>Media Storage</td>
<td>Optional</td>
</tr>
<tr>
<td>MP-5</td>
<td>Media Transport</td>
<td>Optional</td>
</tr>
<tr>
<td>MP-6</td>
<td>Media Sanitization</td>
<td>MP-6</td>
</tr>
<tr>
<td>MP-7</td>
<td>Media Use</td>
<td>MP-7 (1)</td>
</tr>
<tr>
<td>MP-8</td>
<td>Media Downgrading</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td><strong>Physical and Environmental Protection</strong></td>
<td></td>
</tr>
<tr>
<td>PE-1</td>
<td>Physical and Environmental Protection</td>
<td>PE-1</td>
</tr>
<tr>
<td>PE-2</td>
<td>Physical Access Authorizations</td>
<td>PE-2</td>
</tr>
<tr>
<td>PE-3</td>
<td>Physical Access Control</td>
<td>PE-3</td>
</tr>
<tr>
<td>PE-4</td>
<td>Access Control for Transmission Medium</td>
<td>PE-4</td>
</tr>
<tr>
<td>PE-5</td>
<td>Access Control for Output Devices</td>
<td>Optional</td>
</tr>
<tr>
<td>PE-6</td>
<td>Monitoring Physical Access</td>
<td>PE-6 (1)</td>
</tr>
<tr>
<td>PE-8</td>
<td>Visitor Access Records</td>
<td>PE-8</td>
</tr>
<tr>
<td>PE-9</td>
<td>Power Equipment and Cabling</td>
<td>Optional</td>
</tr>
<tr>
<td>PE-10</td>
<td>Emergency Shutoff</td>
<td>Optional</td>
</tr>
<tr>
<td>PE-11</td>
<td>Emergency Power</td>
<td>Optional</td>
</tr>
<tr>
<td>PE-12</td>
<td>Emergency Lighting</td>
<td>PE-12</td>
</tr>
<tr>
<td>PE-13</td>
<td>Fire Protection</td>
<td>PE-13</td>
</tr>
<tr>
<td>PE-14</td>
<td>Temperature and Humidity Controls</td>
<td>PE-14</td>
</tr>
<tr>
<td>PE-15</td>
<td>Water Damage Protection</td>
<td>PE-15</td>
</tr>
<tr>
<td>PE-16</td>
<td>Delivery and Removal</td>
<td>PE-16</td>
</tr>
<tr>
<td>PE-17</td>
<td>Alternate Work Site</td>
<td>Optional</td>
</tr>
<tr>
<td>PE-18</td>
<td>Location of Information System Components</td>
<td>Optional</td>
</tr>
<tr>
<td>PE-19</td>
<td>Information Leakage</td>
<td>Optional</td>
</tr>
<tr>
<td>PE-20</td>
<td>Asset Monitoring and Tracking</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td><strong>Planning</strong></td>
<td></td>
</tr>
<tr>
<td>PL-1</td>
<td>Security Planning Policy and Procedures</td>
<td>Optional</td>
</tr>
<tr>
<td>PL-2</td>
<td>System Security Plan</td>
<td>Optional</td>
</tr>
<tr>
<td>PL-4</td>
<td>Rules of Behavior</td>
<td>PL-4</td>
</tr>
<tr>
<td>PL-5</td>
<td>Privacy Impact Assessment</td>
<td>Optional</td>
</tr>
<tr>
<td>PL-7</td>
<td>Security Concept of Operations</td>
<td>Optional</td>
</tr>
<tr>
<td>PL-8</td>
<td>Information Security Architecture</td>
<td>PL-8</td>
</tr>
<tr>
<td>PL-9</td>
<td>Central Management</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td><strong>Personnel Security</strong></td>
<td></td>
</tr>
<tr>
<td>PS-1</td>
<td>Personnel Security Policy and Procedures</td>
<td>PS-1</td>
</tr>
<tr>
<td>PS-2</td>
<td>Position Risk Designation</td>
<td>PS-2</td>
</tr>
<tr>
<td>PS-3</td>
<td>Personnel Screening</td>
<td>PS-3</td>
</tr>
<tr>
<td>CNTL NO.</td>
<td>CONTROL NAME</td>
<td>INITIAL CONTROL BASELINES</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LOW</td>
</tr>
<tr>
<td>PS-4</td>
<td>Personnel Termination</td>
<td>PS-4</td>
</tr>
<tr>
<td>PS-5</td>
<td>Personnel Transfer</td>
<td>PS-5</td>
</tr>
<tr>
<td>PS-6</td>
<td>Access Agreements</td>
<td>PS-6</td>
</tr>
<tr>
<td>PS-7</td>
<td>Third-Party Personnel Security</td>
<td>PS-7</td>
</tr>
<tr>
<td>PS-8</td>
<td>Personnel Sanctions</td>
<td>PS-8</td>
</tr>
<tr>
<td></td>
<td>Risk Assessment</td>
<td></td>
</tr>
<tr>
<td>RA-1</td>
<td>Risk Assessment Policy and Procedures</td>
<td>RA-1</td>
</tr>
<tr>
<td>RA-2</td>
<td>Security Categorization</td>
<td>RA-2</td>
</tr>
<tr>
<td>RA-3</td>
<td>Risk Assessment</td>
<td>RA-3</td>
</tr>
<tr>
<td>RA-4</td>
<td>Risk Assessment Update</td>
<td>Incorporated into RA-3</td>
</tr>
<tr>
<td>RA-5</td>
<td>Vulnerability Scanning</td>
<td>RA-5</td>
</tr>
<tr>
<td>RA-6</td>
<td>Technical Surveillance Countermeasures Survey</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>System and Services Acquisition</td>
<td></td>
</tr>
<tr>
<td>SA-1</td>
<td>System and Services Acquisition</td>
<td>SA-1</td>
</tr>
<tr>
<td>SA-2</td>
<td>Allocation of Resources</td>
<td>SA-2</td>
</tr>
<tr>
<td>SA-3</td>
<td>System Development Life Cycle</td>
<td>SA-3</td>
</tr>
<tr>
<td>SA-4</td>
<td>Acquisition Process</td>
<td>SA-4 (10)</td>
</tr>
<tr>
<td>SA-5</td>
<td>Information System Documentation</td>
<td>SA-5</td>
</tr>
<tr>
<td>SA-8</td>
<td>Security Engineering Principles</td>
<td>Optional</td>
</tr>
<tr>
<td>SA-9</td>
<td>External Information System Services</td>
<td>SA-9</td>
</tr>
<tr>
<td>SA-10</td>
<td>Developer Configuration Management</td>
<td>Optional</td>
</tr>
<tr>
<td>SA-11</td>
<td>Developer Security Testing and Evaluation</td>
<td>Optional</td>
</tr>
<tr>
<td>SA-12</td>
<td>Supply Chain Protection</td>
<td>Optional</td>
</tr>
<tr>
<td>SA-13</td>
<td>Trustworthiness</td>
<td>Optional</td>
</tr>
<tr>
<td>SA-14</td>
<td>Criticality Analysis</td>
<td>Optional</td>
</tr>
<tr>
<td>SA-15</td>
<td>Development Process, Standards, and Tools</td>
<td>Optional</td>
</tr>
<tr>
<td>SA-16</td>
<td>Developer-Provided Training</td>
<td>Optional</td>
</tr>
<tr>
<td>SA-17</td>
<td>Developer Security Architecture and Design</td>
<td>Optional</td>
</tr>
<tr>
<td>SA-18</td>
<td>Tamper Resistance and Detection</td>
<td>Optional</td>
</tr>
<tr>
<td>SA-19</td>
<td>Component Authenticity</td>
<td>Optional</td>
</tr>
<tr>
<td>SA-20</td>
<td>Customized Development of Critical Components</td>
<td>Optional</td>
</tr>
<tr>
<td>SA-21</td>
<td>Developer Screening</td>
<td>Optional</td>
</tr>
<tr>
<td>SA-22</td>
<td>Unsupported System Components</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>System and Communications Protection</td>
<td></td>
</tr>
<tr>
<td>SC-1</td>
<td>System and Communications Protection Policy and Procedures</td>
<td>SC-1</td>
</tr>
<tr>
<td>SC-2</td>
<td>Application Partitioning</td>
<td>SC-2</td>
</tr>
<tr>
<td>SC-3</td>
<td>Security Function Isolation</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-4</td>
<td>Information in Shared Resources</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-5</td>
<td>Denial of Service Protection</td>
<td>SC-5</td>
</tr>
<tr>
<td>CNTL NO.</td>
<td>CONTROL NAME</td>
<td>INITIAL CONTROL BASELINES</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LOW</td>
</tr>
<tr>
<td>SC-6</td>
<td>Resource Availability</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-7</td>
<td>Boundary Protection</td>
<td>SC-7</td>
</tr>
<tr>
<td>SC-8</td>
<td>Transmission Confidentiality and Integrity</td>
<td>SC-8</td>
</tr>
<tr>
<td>SC-10</td>
<td>Network Disconnect</td>
<td>SC-10</td>
</tr>
<tr>
<td>SC-11</td>
<td>Trusted Path</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-12</td>
<td>Cryptographic Key Establishment and Management</td>
<td>SC-12</td>
</tr>
<tr>
<td>SC-13</td>
<td>Cryptographic Protection</td>
<td>SC-13</td>
</tr>
<tr>
<td>SC-16</td>
<td>Transmission of Security Attributes</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-17</td>
<td>Public Key Infrastructure Certificates</td>
<td>SC-17</td>
</tr>
<tr>
<td>SC-18</td>
<td>Mobile Code</td>
<td>SC-18</td>
</tr>
<tr>
<td>SC-19</td>
<td>Voice Over Internet Protocol</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-20</td>
<td>Secure Name /Address Resolution Service (Authoritative Source)</td>
<td>SC-20</td>
</tr>
<tr>
<td>SC-21</td>
<td>Secure Name /Address Resolution Service (Recursive or Caching Resolver)</td>
<td>SC-21</td>
</tr>
<tr>
<td>SC-22</td>
<td>Architecture and Provisioning for Name/Address Resolution Service</td>
<td>SC-22</td>
</tr>
<tr>
<td>SC-23</td>
<td>Session Authenticity</td>
<td>SC-23</td>
</tr>
<tr>
<td>SC-24</td>
<td>Fail in Known State</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-25</td>
<td>Thin Nodes</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-26</td>
<td>Honeypots</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-27</td>
<td>Platform-Independent Applications</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-28</td>
<td>Protection of Information at Rest</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-29</td>
<td>Heterogeneity</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-30</td>
<td>Concealment and Misdirection</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-31</td>
<td>Covert Channel Analysis</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-32</td>
<td>Information System Partitioning</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-34</td>
<td>Non-Modifiable Executable Programs</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-35</td>
<td>Honeyclients</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-36</td>
<td>Distributed Processing and Storage</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-37</td>
<td>Out-of-Band Channels</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-38</td>
<td>Operations Security</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-39</td>
<td>Process Isolation</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-40</td>
<td>Wireless Link Protection</td>
<td>SC-40</td>
</tr>
<tr>
<td>SC-41</td>
<td>Port and I/O Device Access</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-42</td>
<td>Sensor Capability and Data</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-43</td>
<td>Usage Restrictions</td>
<td>Optional</td>
</tr>
<tr>
<td>SC-44</td>
<td>Detonation Chambers</td>
<td>Optional</td>
</tr>
</tbody>
</table>

**System and Information Integrity**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SI-1</td>
<td>System and Information Integrity Policy and Procedures</td>
<td>SI-1</td>
</tr>
<tr>
<td>SI-2</td>
<td>Flaw Remediation</td>
<td>SI-2</td>
</tr>
<tr>
<td>SI-3</td>
<td>Malicious Code Protection</td>
<td>SI-3</td>
</tr>
<tr>
<td>CNTL NO.</td>
<td>CONTROL NAME</td>
<td>INITIAL CONTROL BASELINES</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>SI-4</td>
<td>Information System Monitoring</td>
<td>SI-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SI-4 (2) (4) (5)</td>
</tr>
<tr>
<td>SI-5</td>
<td>Security Alerts, Advisories, and Directives</td>
<td>SI-5</td>
</tr>
<tr>
<td>SI-6</td>
<td>Security Function Verification</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td>SI-7</td>
<td>Software, Firmware, and Information Integrity</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SI-7 (1) (7)</td>
</tr>
<tr>
<td>SI-8</td>
<td>Spam Protection</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SI-8 (1) (2)</td>
</tr>
<tr>
<td>SI-10</td>
<td>Information Input Validation</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SI-10</td>
</tr>
<tr>
<td>SI-11</td>
<td>Error Handling</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SI-11</td>
</tr>
<tr>
<td>SI-12</td>
<td>Information Handling and Retention</td>
<td>SI-12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SI-12</td>
</tr>
<tr>
<td>SI-13</td>
<td>Predictable Failure Prevention</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td>SI-14</td>
<td>Non-Persistence</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td>SI-15</td>
<td>Information Output Filtering</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td>SI-16</td>
<td>Memory Protection</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SI-16</td>
</tr>
<tr>
<td>SI-17</td>
<td>Fail-Safe Procedures</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional</td>
</tr>
</tbody>
</table>
SECTION 2. IMPLEMENTATION AND MANAGEMENT

This Manual is the foundation for information technology security in state government and is required for all executive branch agencies to follow in order to comply with statewide information security standards. To be successful, Agency leadership must continue to emphasize the importance of information security throughout their organizations and at their discretion, implement additional supplementary controls as deemed necessary. When considering the supplementary controls not included in the State’s policies, agencies should refer to NIST SP 800-53 Rev 4 and industry security practices related to information technology implementation. Agencies are also required to ensure ongoing compliance by implementing continuous monitoring activities.

SECTION 3 – INFORMATION PROTECTION

 Agencies must implement appropriate safeguards as defined in the supporting policy documents (such as identification and authentication, encryption, data filtering, tagging, Multi-factor authentication or segregation) to ensure Restricted and Highly Restricted information, including Personally Identifiable Information (PII), Federal Tax Information (FTI), Payment Card Industry (PCI) is protected from inappropriate disclosure, misuse, or other security breaches, in accordance with State, Federal and other security standards and requirements. Agencies must ensure an appropriate response in the event of a breach of sensitive PII consistent with Federal and Agency standards and requirements.

SECTION 4 – CONTINUOUS MONITORING

Continuous monitoring, automatic alerting, and auditing with corresponding tracking capabilities and reporting are required for devices connected to the State infrastructure or supporting State business (e.g. cloud services). Agencies must also have procedures in place to ensure robust incident response to unauthorized accesses and activities. The State CIO has the authority to require the installation of monitoring or auditing agents on devices connected to the network.

SECTION 5 – SECURITY ARCHITECTURE

 Agencies must implement appropriate information safeguards (such as encryption, data filtering, tagging, or segregation) to ensure highly restricted information, including Personally Identifiable Information (PII), Federal Tax Information (FTI), Payment Card Industry (PCI) is protected from inappropriate disclosure, misuse, or other security breaches, in accordance with State, Federal and other security standards and requirements. Agencies must ensure an appropriate response in the event of a breach of sensitive PII consistent with Federal and Agency standards and requirements.

SECTION 4 – REFERENCES

The following policies in the Statewide Information Security Manual provide additional details for the implementation of State information technology resources.

- SCIO-SEC-301: Access Control Policy (AC)
- SCIO-SEC-302: Awareness and Training Policy (AT)
- SCIO-SEC-303: Audit and Accountability Policy (AU)
- SCIO-SEC-304: Security Assessment and Authorization Policy (CA)
- SCIO-SEC-305: Configuration Management Policy (CM)
- SCIO-SEC-306: Contingency Planning Policy (CP)
- SCIO-SEC-307: Identification and Authentication Policy (IA)
- SCIO-SEC-308: Incident Response Policy (IR)
- SCIO-SEC-309: Maintenance Policy (MA)
- SCIO-SEC-310: Media Protection Policy (MP)
- SCIO-SEC-311: Personnel Security Policy (PS)
- SCIO-SEC-312: Security Planning Policy (PL)
- SCIO-SEC-313: Physical and Environmental Protection Policy (PE)
- SCIO-SEC-314: Risk Assessment Policy (RA)
- SCIO-SEC-315: System and Services Acquisition Policy (SA)
- SCIO-SEC-316: System and Communications Protection Policy (SC)
- SCIO-SEC-317: System and Information Integrity Policy (SI)