	System and Communications Protection Policy	Document No. SCIO-SEC-316

Effective Date	Review Date	Version	Page No.
01/29/2018	03/26/2025	4	1 of 21

Scope

The Statewide Information Security Policies are the foundation for information technology security in North Carolina. The policies set 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. This policy covers all State information and information systems to include those used, managed, or operated by a contractor, an agency, or other organization on behalf of the State. This policy applies to all State employees, contractors, and all other users of State information and information systems that support the operation and assets of the State. 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. This security policy is consistent with applicable laws, executive orders, directives, regulations, other policies, standards, and guidelines.

Material Superseded

This current policy supersedes all previous versions of the policy. All State agencies and vendors of the State are expected to comply with the current implemented version of this policy.

Responsibilities

All covered personnel involved in the implementation or operation of system and communications protection controls are responsible for adhering to this policy and with any additional local system and communications protection requirements.

Role	Definition
Agency Management	The Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designated organizational officials at the senior leadership level are assigned the responsibility for documenting, disseminating, and implementing a secure information system and communications protection program throughout the agencies.
Agency Security Liaison	The Agency Security Liaison is responsible for ensuring that information system and service acquisition requirements are managed in compliance with the State's requirements by collaborating with organizational entities. Liaisons are responsible for maintaining the appropriate information system and communications protection required for information security protection.
Information System Owner	The Information System Owner (SO) is responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Third Parties	Third party service providers are responsible for ensuring that systems, system components and services they provide are secure and do not negatively impact security of pre-existing systems by implementing secure information system and communications protection practices in accordance with this policy.

SC-1 – Policy and Procedures

All information assets that process, store, receive, transmit or otherwise could impact the confidentiality, integrity, and accessibility of State data must meet the required security controls defined in this policy document that are based on the National Institute of Standards and Technology (NIST) SP 800-53, Security and Privacy Controls. This document addresses the procedures and standards set forth by the State to implement the family of System and Communications Protection security controls at the organization, process and/or system level for all information assets / State data.

The State has adopted the System and Communications Protection security principles established in NIST SP 800-53, "System and Communications Protection" control guidelines as the official policy for this security domain. The "SC" designator identified in each control represents the NIST-specified identifier for the System and Communications Protection control family. The following subsections in this document outline the System and Communications Protection requirements that each agency shall implement and maintain in order to protect the confidentiality, integrity and availability of information and information systems by assuring systems, system components and services acquired are secure and do not negatively impact security of pre-existing systems used for conducting the agencies' mission critical business functions.

This policy and associated procedures shall be reviewed and updated annually, at a minimum. They shall also be updated following agency-defined events that necessitate such change.

This policy and the associated procedures shall be developed, documented, and disseminated by the Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designated organizational officials at the senior leadership level.

SC-2 – Separation of System and User Functionality

User functionality (including user interface services) shall be separated from information system management functionality in application components.

a. For the Application and Database secure zones, an approved firewall or other network segmentation mechanism, for example micro segmentation or virtual local area networks (VLANs), is required to segregate application servers and database servers.

b. Information systems shall prevent the presentation of information system management-related functionality at an interface for non-privileged users.

c. Internal network infrastructures (e.g., local area networks [LANs]) shall be segregated into network zones to protect application servers from the user LAN.

d. Production and non-production environments (e.g., test, development, QA, etc.) shall be segregated from one another.

e. Wireless networks shall be physically or logically segregated from internal networks such that an unknown external user cannot access an agency's internal network.

f. Systems not able to adhere to the DMZ and/or other security requirements of this policy need to be in a Special Assembly zone. Agencies must document the rationale for developing a Special Assembly zone.

i. An example of special assembly zones includes facility management systems, such as heating, ventilation, or air conditioning (HVAC), badge access, electrical generators, power distribution, water, and closed-circuit television (CCTV). These may be excluded from the network zoning requirements, provided those systems are not publicly accessible, are logically isolated (e.g., VLANs) from other networked systems and cannot access other shared systems/services, and have appropriate access control mechanisms in place.

g. Where technically configurable, virtual machines with Highly Restricted data shall be separated from those with unrestricted data.

SC-3 – Security Function Isolation (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-4 - Information in Shared System Resources

Information systems shall prevent unauthorized and unintended information transfer via shared system resources.

a. Information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) shall not be made available for object reuse or shall residual information be made available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems.

b. Information systems shall prevent unauthorized information transfer via shared resources in accordance with statewide information security standards when system processing explicitly switches between different information classification levels or security categories.

c. This control is optional for LOW risk information systems.

SC-5 – Denial of Service Protection

The effects of denial of service (DoS) attacks shall be limited by appropriately securing all hosts that could be a potential target for a common DoS or a distributed denial of service (DDoS) attack. The following controls shall be implemented:

a. Denying all inbound traffic by default, thus limiting the channels of network attacks;

b. Periodically scanning network and devices for bots (software robots) and Trojan horse programs;

c. Deploying authentication mechanisms wherever technically configurable;

d. Designing and implementing networks for maximum resiliency;

e. Developing specific plans for responding to DoS and DDoS attacks in the agency incident management plan and the business continuity plan;

f. Managing excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks;

g. 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.

h. Additional guidance is available NIST SP 800-61 Computer Security Incident Handling Guide.

SC- 6 – Resource Availability (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-7 – Boundary Protection

The following shall be done for boundary protection:

a. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with statewide security architecture and privacy 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).

b. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system.

c. Implement subnetworks for publicly accessible system components that are physically and logically separated from internal agency network.

d. 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.

e. 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").

f. 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.

g. Firewalls shall be configured to the following specifications:

   i. Local user accounts shall be configured on network firewalls, for the sole purpose of eliminating possible extended outages.

   ii. Local accounts shall be configured to only be used when the device cannot make contact with the central unit. During normal operation, the local account exists, but is not used.

   iii. 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.

   iv. 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 rule set changes are approved and implemented.

   v. For temporary or emergency port openings, the process shall establish a maximum time for the port to be open, which shall not exceed 5 days. The authorized firewall rule set administrators, or the entity managing the firewall, shall subsequently close the port or develop additional hardening.

   vi. 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.

   vii. Firewalls shall be installed in locations that are physically secure from tampering. Firewalls shall not be relocated without the prior approval of agency management.

   viii. Firewall rule sets shall always block the following types of network traffic:

      a) Unauthorized scanning activity that originates outside of its network, within its network, and between information systems.

      b) Inbound network traffic from a non-authenticated source system with a destination address of the firewall system itself.

      c) Inbound network traffic with a source address indicating that the packet originated on a network behind the firewall.

      d) 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.

e) Inbound network traffic containing IP Source Routing information.

f) Inbound or outbound network traffic containing a source or destination address of 0.0.0.0 and/or containing directed broadcast addresses.

ix. 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.

x. Firewall rule implementation shall have an approval process that includes review by the Security Liaison, or designated personnel, of the agency that requires or no longer requires the rule. Existing firewall rules shall be reviewed every 6 months by the Security Liaison, or designated personnel, that is responsible for the application/device that requires the rule sets in question. For example, agency X application requires certain firewall rules to be implemented; therefore, that agency security liaison is responsible for approving and reviewing the firewall rules required for the application. Confirmation of the firewall rule review that is conducted every 6 months shall be sent to the ESRMO.

xi. Additional requirements for protecting Federal Tax Information (FTI) on networks are provided in IRS 1075 Section 3.3.6 Network Boundary and Infrastructure.

xii. 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).

h. NIST SP 800-41 must be used as guidance on firewalls and firewall rule set.

i. NIST SP 800-189 must be used as guidance on routers.

j. NIST SP 800-77 must be used as guidance on Virtual Private Networks (VPNs).

k. NIST SP 800-94 must be used as guidance on IDPS.

SC-7 (4) – Boundary Protection | External Telecommunications Services

The following shall be done:

a. Implement a managed interface for each external telecommunication service.

b. Establish a traffic flow policy for each managed interface.

c. Protect the confidentiality and integrity of the information being transmitted across each interface.

d. Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need.

e. Review exceptions to the traffic flow policy annually and remove exceptions that are no longer supported by an explicit mission/business need.

f. Prevent unauthorized exchange of control plane traffic with external network.

g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks.

SC-7 (5) – Boundary Protection | Deny by Default – Allow By exception

Protective controls shall at a minimum include the following:

a. Positive source and destination address checking to restrict rogue networks from manipulating the State's routing tables.

b. Firewalls must use an authentication mechanism that provides accountability for the individual and to ensure device configuration does not become corrupted with false entries.

c. Screen internal network addresses from external view.

d. Information systems at managed interfaces shall deny network communications traffic by default and allow network communications traffic by exception (e.g., deny all, permit by exception, also known as whitelisting). 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.

SC- 7 (7) – Boundary Protection | Split Tunneling for Remote Devices

Information systems, in conjunction with a remote device, shall prevent the device from simultaneously establishing non-remote connections (e.g., split tunneling) with the system and communicating via some other connection to resources in external networks.

SC-7 (8) – Boundary Protection | Route Traffic to Authenticated Proxy Servers

Where technically configurable, routing agency-defined internal communications traffic to agency-defined external networks shall be achieved through authenticated proxy servers at managed interfaces, such as web content filtering devices.

SC-8 – Transmission Confidentiality and Integrity

The confidentiality and integrity of transmitted information shall be protected during the transfer process.

a. Organizations 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. The organization must ensure that all network infrastructure, access points, wiring, conduits, and cabling are within the control of authorized personnel.

b. Network monitoring capabilities must be implemented to detect and monitor for suspicious network traffic.

c. Controls shall be deployed to ensure resources do not contribute to outside-party attacks. These controls include the following:

   i. Securing interfaces between agency-controlled and non-agency-controlled or public networks.

   ii. Standardizing authentication mechanisms in place for both users and equipment.

   iii. Controlling users' access to information resources.

   iv. Monitoring for anomalies or known signatures via intrusion detection systems (IDS) and/or intrusion prevention systems (IPS). IDPS signatures shall be up to date.

d. Employees, contractors, and others performing work for the State shall not intercept or attempt to intercept data transmissions of any kind that they are not authorized to access.

e. Employees, contractors, and others performing work for the State shall not use any utility, application, or service on a device used to access State systems that obfuscates or anonymizes user or device identity (e.g., IP address, MAC address, user identity, geographic location, etc.), except for authorized State-managed solutions. Prohibited services include, but are not limited to, the following: personal VPN, anonymizing/privacy features of a device or software, Private Relay, and Tor.

f. 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.

g. Organizations 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.

h. Secure protocols, such as Secure Shell (SSH), Transport Layer Security (TLS), and Internet Protocol Security (IPSec) shall be used for secure network management functions.

i. All communications that transfer confidentially sensitive data between web clients and web servers must employ the most current secure transport protocol version(s) utilizing TLS as per NIST SP 800-52 Rev 2. Any TLS version that is disallowed, or not otherwise covered with a 'shall' and

'should' or has reached the end of a deprecation period as per NIST SP 800-52 Rev. 2 shall not be utilized.

j. NIST SP 800-52 Rev. 2 must be used as guidance on protecting transmission integrity using TLS.

k. NIST SP 800-77 must be used as guidance on protecting transmission integrity using IPsec.

l. NIST SP 800-81 must be used as guidance on Domain Name System (DNS) message authentication and integrity verification.

m. NIST SP 800-113 must be used as guidance on SSL VPNs.

n. Instant messaging technologies, where allowed, must not be used to transmit any type of Restricted or Highly Restricted data.

o. The following types of transmission require enhanced protection (e.g., cryptography mechanisms) when integrity is an important consideration:

   i. Internal traffic within the information system and applications

   ii. Internal traffic between two or more information systems

   iii. External traffic to or across the Internet

   iv. Remote access

   v. Email

   vi. FTP transmissions

   vii. Web services

   viii. Voice over Internet Protocol (VoIP)

   ix. Audio and video

   x. Wireless client to host communications

p. Agencies shall protect the confidentiality of data transmitted on the network from corruption or data loss by prohibiting the extending, modifying, or retransmitting network services, such as through the installation of new switches or other network devices, unless prior Agency CIO or delegate approval is granted.

SC-8 (1) – Transmission Confidentiality and Integrity | Cryptographic Protection

Cryptographic mechanisms shall be implemented to prevent unauthorized disclosure of information and/or to detect changes to information during transmission.

SC-9 – Transmission Confidentiality

Withdrawn: Incorporated into SC-8

SC-10 – Network Disconnect

a. All sessions shall be terminated that have had no activity for a period of thirty (30) minutes or less, such that the user must re-authenticate his/her identity to resume the session.

b. An absolute time-out shall occur after twenty-four (24) hours of continuous connection and shall require reconnection and authentication to re-enter the State Network.

c. The information system must be configured to disconnect inactive remote VPN.

SC-11 – Trusted Path (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-12 – Cryptographic Key Establishment and Management

Electronic key systems shall be managed according to the following requirements:

a. FIPS 140-2, or 140-3 where available, approved algorithms that do not have any known weaknesses shall be used when protecting Restricted or Highly Restricted data. Enablement of full FIPS mode in an application or operating system is not required. Organizations may optionally enable additional cipher algorithms for transport encryption if they are not considered legacy or disallowed by FIPS and do not have any known weakness. Known weaknesses are things such as, but not limited to, less than 128-bit for ciphers, weak configuration parameters that affect the whole, or a vulnerability. The following is provided as a quick reference list for common FIPS approved algorithms at the time of this writing:

   i. Block cipher algorithms: AES-128, AES-192, AES-256
   ii. Digital Signatures: RSA ≥ 2048, ECDSA or EdDSA ≥ 224
   iii. Hash functions: SHA-2 family (e.g., SHA-256), SHA-3 family (e.g. SHA3-256), TupleHash/ParallelHash only as per SP 800-185.

   Products and modules that have been validated by NIST as FIPS 140-2 compliant and are currently listed as validated products list may be found at http://csrc.nist.gov/groups/STM/cmvp/validation.html.

b. Key-based data encryption systems must implement a key escrow system to guarantee access to encrypted data when needed. Key escrow data shall be routinely backed up. Recovery procedures must be tested at least annually to ensure access and availability to encrypted data.

c. Only authorized personnel shall have access to keys used to access Restricted or Highly Restricted data. Encryption keys must be properly stored (separate from data) and available, if needed, for later decryption. The following must also be ensured:

   i. Separation of duties or dual control procedures are enforced.

   ii. Any theft or loss of electronic keys results in the notification of management.

   iii. All keys are protected against modification, substitution, and destruction, and secret/private keys are protected against unauthorized disclosure.

   iv. Cryptographic keys are replaced or retired when keys have reached the end of their life or the integrity of the key has been weakened or compromised.

   v. Physical protection is employed to protect equipment used to synchronize, store and archive keys.

   vi. An electronic key management and recovery system, including all relevant key escrow procedures, is documented and in place. This shall be handled through key escrow procedures.

   vii. Custodians of cryptographic keys formally acknowledge they understand and accept their key-custodian responsibilities.

   viii. Encrypted data are recoverable, at any point in time, even when the person(s) who encrypted the data is no longer available.

d. NIST SP 800-56A and NIST SP 800-56B must be referenced as procedures, on establishing cryptographic keys.

e. NIST SP 800-57 must be referenced as guidance on managing cryptographic keys.

SC-13 – Cryptographic Protection

Cryptographic modules must be implemented for cryptographic uses as described below. Cryptographic requirements for each specified cryptographic use shall be defined:

a. All laptops that are used to conduct State business shall use encryption to protect all information stored on the laptop's storage device.

b. All other mobile computing devices and portable computing devices such as smart phones, tablets, and portable storage devices such as compact disks (CDs), digital video disks (DVDs), media players (MP3 players) and flash drives that are used to conduct State business, shall use encryption to protect all Restricted and Highly Restricted data from unauthorized disclosure.

Device	Encryption Requirements
Laptops, Notebooks, etc.	All devices shall use Full Disk Encryption (FDE) using a FIPS 140-2 Level 1 certified AES-256 encryption algorithm.
Mobile and portable computing devices, such as tablets, smart phones, and personal digital assistants. Removable Media such as CDs, DVDs, memory sticks (flash drives), tape media, or any other	All Restricted or Highly Restricted data shall be encrypted using a FIPS 140-2 Level 1 certified algorithm of at least 128-bit strength. **Note**: Restricted and Highly Restricted State data should only be stored on State issued and State-owned media.

c. Policies concerning the storage of the State's Restricted and Highly Restricted data on all portable and removable media devices shall be enforced.

d. For a list of validated cryptographic modules and products, refer to the following NIST publication: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm.

SC-14 – Public Access Protections

Withdrawn: Capability provided by AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10.

SC-15 – Collaborative Computing Devices and Applications

The following shall be done when using collaborative computing devices and applications:

a. Prohibit remote activation of collaborative computing devices and applications, for example, networked white boards, cameras, and microphones.

b. Provide an explicit indication of use to users physically present at the devices. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

SC-16 – Transmission of Security and Privacy Attributes (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-17 – Public Key Infrastructure Certificates

a. Public key infrastructure certificates shall be issued or obtained from an approved service provider.

b. Registration to receive a public key certificate must include authorization by a supervisor or a responsible official.

c. Public key certificates must be issued by using a secure process that both verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

d. Organizations shall include only approved trust anchors in trust stores or certificate stores managed by the organization.

e. Only digital certificates for transport encryption either issued by and/or approved by the State Certification Authority (managed by NCDIT) can be used on end-user facing State applications and/or systems as well as for system-to-system where external connections are accepted. For internal system-to-system transport encryption, internally signed certificates may be utilized so long as at minimum they adhere to algorithm requirements in SC-12(a), are valid for no longer than four years, and can be tracked and managed to prevent expiration.

f. NIST SP 800-32 must be used as guidance on public key technology.

g. NIST SP 800-63, Version 1.0.2 must be used as guidance on remote electronic authentication.

SC-18 – Mobile Code

A tamper protection program shall be implemented for the information system, system component, or information system service to protect the State Network from mobile code that performs unauthorized and malicious actions. Refer to the Statewide Glossary of IT Terms for a definition of mobile code. The following are categories of mobile code/active content:

a. Category 1/high risk mobile code technologies exhibit a broad functionality, allowing unmediated access to workstation, server and remote system services and resources. These pose a significant risk to the State's information systems because they allow unlimited access to a user's computer. There are two subgroups of Category 1 mobile code technologies:

   i. Category 1 technologies can differentiate between signed and unsigned mobile code. The technologies can also be configured to allow the execution of signed mobile code while simultaneously blocking the execution of unsigned mobile code. Category 1 mobile code technologies may be used by agencies when additional restrictions are implemented. The following are assigned to Category 1:

      - ActiveX controls
      - Shockwave movies (e.g., dcr, .dxr, .dir files), including Xtras, that execute in the Shockwave for Director plug-in.

   ii. Category 1 consists of mobile code technologies that are prohibited from use on State information systems beyond the local information system's authorization boundary, or to or from external entities because they cannot differentiate between signed and unsigned mobile code, nor can they be configured to block the execution of unsigned mobile code while enabling the execution of signed mobile code. The following are assigned to Category 1:

- Mobile code scripts that execute in Windows Scripting Host (WSH) (e.g., JavaScript or VBScript downloaded via URL file reference or email attachments)
- Hypertext Mark-up Language (HTML) applications (e.g., .hta files) that download as mobile code
- Scrap objects (e.g., .shs and .shb files)
- Microsoft Disk Operating System (MS-DOS) batch scripts
- UNIX shell scripts
- Binary executables (e.g., .exe files) that download as mobile code

ii. Category 1 mobile code must be obtained from a trusted source and must be signed with a State approved PKI code-signing certificate.

iii. All information systems capable of executing mobile code must be configured to disable the execution of unsigned Category 1 mobile code obtained from outside the organization-managed boundary.

b. Category 2/medium risk mobile code technologies have full functionality, allowing mediated or controlled access to workstations, server, and remote system services and resources. Category 2 technologies can pose a moderate security threat to the State's information systems because they offer limited control by the user on what the code is allowed to do. They may be used when the Category 2 restrictions described in Section 6, Procedures are implemented.

i. The following are assigned to Category 2:

- Java applets and other Java mobile code
- Visual Basic for Applications (VBA) (e.g., Microsoft Office macros)
- LotusScript (e.g., Lotus Notes scripts)
- PerfectScript (e.g., Corel Office macros)
- Postscript
- Mobile code executing in .NET Common Language Runtime

ii. Category 2 mobile code may be used if it is obtained from a trusted source over an assured channel (i.e., TLS VPN, IPsec, or other approved by the ESRMO).

iii. Unsigned Category 2 code, whether or not obtained from a trusted source over an assured channel, may be used if it executes in a constrained environment without access to local system and network resources (e.g., file system, Windows registry, or network connections other than to its originating host).

iv. Where technically configurable, web browsers and other mobile code-enabled products must be configured to prompt the user prior to the execution of Category 2 code.

v. Where technically configurable, protections against malicious Category 2 technologies must be employed at end user systems and at system boundaries.

c. Category 3/low risk mobile code technologies support limited functionality, with no capability for unmediated access to workstation, server, and remote system services and resources. Category 3 mobile code may be freely used without restrictions in information systems. Category 3 technologies pose limited risk to the State's information systems because they are very restricted in the actions they can perform. The following are assigned to Category 3:

- JavaScript, including Jscript and European Computer Manufacturers Association (ECMA) Script variants, when executing in the browser
- VBScript, when executing in the browser
- Portable Document Format (PDF)
- Flash animations (e.g., .swf and .spl files) that execute in the Shockwave Flash plug-in

d. Emerging mobile code technologies refer to all mobile code technologies, systems, platforms, or languages whose capabilities and threat level have not yet undergone a risk assessment and therefore have not been assigned to one of the three risk categories described above. Emerging mobile code technologies must not be used unless approved by management. The download and execution of mobile code using emerging technologies must be blocked by all means available at the network boundary, workstation, host, and within applications.

SC-19 – Voice Over Internet Protocol

a. Usage restrictions and implementation guidance shall be established for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.

b. The use of VoIP within the information system shall be authorized, monitored, and controlled.

c. This control is optional for LOW risk information systems.

SC-20 – Secure Name/Address Resolution Service (Authoritative Source)

Information systems shall require the following for domain name system (DNS):

a. Enable external clients, including remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service using DNS servers.

b. DNS servers shall not be configured to allow zone transfers to unknown secondary servers.

   i. If an agency maintains a primary DNS server, zone transfers will be allowed only to trusted (known) servers

   ii. If an agency maintains a secondary DNS server, zone transfers will be allowed to the primary DNS server only

   iii. When a domain has a US extension (e.g., state.nc.us), the US Domain Registry requires the domain allow copies to be transferred to the US Domain Registry's Master Server. Therefore, all domains registered with US Domain Registry will allow transfers of copies of their zones to the Master Server for the US Domain Registry. When DIT maintains the DNS, agencies may request DIT to allow additional IP addresses to receive zone transfers. Agencies must work with DIT to define acceptable IP addresses and/or IP address ranges.

SC-21 – Secure Name / Address Resolution Service (Recursive or Caching Resolver)

a. Information systems shall request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources using recursive resolving or caching domain name system (DNS) servers.

b. Recursion on an authoritative name server is prohibited.

SC-22 – Architecture and Provisioning for Name / Address Resolution Service

Information systems that collectively provide name/address resolution service shall be fault-tolerant and implement internal/external role separation.

a. At least two authoritative domain name system (DNS) servers shall be deployed to eliminate single points of failure and to enhance redundancy. One configured as the primary server and the other configured as the secondary server.

b. Servers shall be deployed in two geographically separated network subnetworks (e.g., not located in the same physical facility).

c. Split DNS shall be used to prevent leaking internal system and IP information to external non-State clients to limit information exposure.

d. DNS servers with internal roles shall only process name and address resolution requests from within the organizations (e.g., from internal clients).

e. DNS servers with external roles only process name and address resolution information requests from clients external to organizations (e.g., on external networks including the Internet).

f. Clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists) shall be specified.

g. Servers must be configured to provide redundancy, load balancing and distributed access.

h. NIST SP 800-81 must be used as guidance on secure domain name system deployment.

SC-23 – Session Authenticity

a. Information systems must protect the authenticity of communications sessions. Protection mechanisms shall be selected and implemented to ensure adequate protection of data integrity, confidentiality, and session authenticity in transmission. Mechanisms include but are not limited to the following:

- Security services based on IPsec
- VPNs
- TLS
- DNS
- SSH
- Digital signatures
- Digital certificates
- Digital time stamping
- FIPS 140-2 approved encryption technology

b. Information systems shall invalidate session identifiers upon user logout or other session termination to curtail the ability of adversaries from capturing and continuing to employ previously valid session IDs.

c. NIST SP 800-52 Rev. 2 must be used as guidance on the use of TLS mechanisms.

d. NIST SP 800-77 must be used as guidance on the deployment of IPsec VPNs and other methods of protecting communications sessions.

e. NIST SP 800-95 must be used as guidance on securing web services.

f. NIST SP 800-113 must be used as guidance on SSL VPNs.

SC-24 – Fail in Known State (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-25 – Thin Nodes (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-26 – Decoys (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-27 – Platform-Independent Applications (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-28 – Protection of Information at Rest

Information systems shall protect the confidentiality and integrity of all Restricted or Highly Restricted data at rest. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems.

This control is optional for LOW risk information systems.

SC-28 (1) – Protection of Information at Rest – Cryptographic Protection

a. Cryptographic mechanisms shall be implemented to prevent unauthorized disclosure and modification of all Restricted or Highly Restricted data at rest: Restricted and Highly Restricted data stored in non-volatile storage (e.g., disk drive) on all endpoints shall be encrypted with FIPS 140-2 compliant encryption during storage (regardless of location).

b. Organizations shall consider increasing integrity protection of data by recording data onto hardware-enforced, write-once media. Write-once, read-many (WORM) media includes, for example, Compact Disk-Recordable (CD-R) and Digital Video Disk-Recordable (DVD-R).

c. Organizations shall consider storing data at rest on a physically separate non-mobile storage device (e.g., disk drive, tape drive) with cryptographic protections in place.

d. Whereas a virtual machine may store or process confidential data, the virtual machine image file shall use appropriate controls to protect the data at rest.

e. This control is optional for LOW risk information systems.

SC-29 – Heterogeneity (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-30 – Concealment and Misdirection (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-31 – Covert Channel Analysis (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-32 –System Partitioning (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-33 – Transmission Preparation Integrity

[Withdrawn: Incorporated into SC-8].

SC-34 – Non-Modifiable Executable Programs (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-35 – External Malicious Code Identification (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-36 – Distributed Processing and Storage (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-37 – Out-of-Band Channels (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-38 – Operations Security (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-39 – Process Isolation (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-40 – Wireless Link Protection

The confidentiality of data transmitted on external and internal wireless links shall be protected from corruption or data loss by doing the following.

a. Extending, modifying, or retransmitting network services, such as through the installation of new switches or wireless access points, is prohibited, unless prior approval is granted.

b. Wireless networks shall be physically or logically segregated from internal wired networks such that an unknown external user cannot access an organization's internal network.

c. All Restricted and Highly Restricted data shall be encrypted when transmitted across wireless or public networks, including transmissions such as SFTP and electronic mail. For the encryption requirements of secure transmission of confidential data, refer to SC-13 Cryptographic Protection.

d. All network access points shall be identified and safeguards for the network and individual systems shall be verified as adequate and operational. These systems include wireless access points, network ingress and egress points, and network-attached devices.

e. Use access points that require a key, and which encrypt the wireless communication.

f. Configure wireless LAN settings to not allow automatic joining of any wireless network.

g. For wireless LAN communications, the following encryption settings shall be used:

   i. Depending on the type of information traversing a wireless LAN, encryption is required at varying levels. At a minimum, public information requires Wi-Fi Protected Access (WPA) encryption and Restricted and Highly Restricted data require 802.11i (WPA2)-compliant Advanced Encryption Standard (AES) encryption. End-to-end encryption is highly recommended for the Restricted and Highly Restricted data classification.

   ii. If the Temporal Key Integrity Protocol (TKIP) is the highest level of encryption available for WPA, then WPA2 shall be used.

   iii. When WPA2 is used, AES encryption shall be enabled and shall be no less than 256 bits.

   iv. WPA2 (802.11i) encryption must use TKIP, Counter Mode CBC-MAC Protocol (CCMP), or other IEEE- or NIST-approved key exchange mechanism.

h. When end-to-end encryption is required across both an 802.11 wireless and a wired network, then in addition to WPA2 (802.11i), data transmitted between any wireless devices shall be encrypted using a proven encryption protocol that ensures confidentiality. Such protocols include TLS, SSH, IP Security (IPSec) and VPN tunnels.

SC-41 – Port and I/O Device Access (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-42 – Sensor Capability and Data (Optional)

This control is optional for LOW and MODERATE risk information systems.

SC-43 – Usage Restrictions

Organizations shall do the following regarding usage restrictions:

a. Establish usage restrictions and implementation guidance for information system components including, for example: hardware, software, or firmware components (e.g., VOIP, mobile code, digital copiers, printers, scanners, optical devices, wireless technologies, mobile devices).

b. Define the proper use of information assets through Acceptable User Policies (AUPs) and include critical technologies such as remote access technologies, removable electronic media, laptops, tablets, smartphones, email usage and Internet usage. See the Statewide AUP for further guidance.

SC-44 – Detonation Chambers

Organizations tasked with conducting incident response and forensics, should employ a detonation chamber capability also known as dynamic execution environments in a secure, quarantined environment, to do the following:

a. Allow the opening of email attachments.

b. Allow the execution of untrusted or suspicious applications.

c. Allow the execution of Universal Resource Locator (URL) requests in the safety of an isolated environment or virtualized sandbox to quickly identify malicious code.

d. Reduce the likelihood that the code is propagated to user environments of operation (or prevent such propagation completely).

e. This control is optional for LOW risk information systems.

Enforcement

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.