Division of Enterprise Technology Strategy and Services

ETSS Policy 300.4

System and Communications Protection Policy

Publish Date: 15 July 2026
Effective Date: 15 July 2026
Last Revision Date: 14 July 2026

doa.entsec@doit.ri.gov

1. Purpose

This policy establishes the requirements for protecting State of Rhode Island information systems, networks, and communications to ensure the confidentiality, integrity, and availability of information resources. It defines controls for system segmentation, boundary protection, transmission and data-at-rest encryption, cryptographic key management, network session management, DNS security, and other communications protection mechanisms. This policy maintains the State's defense-in-depth security posture aligned with Zero Trust principles.
This policy supports the State's compliance with NIST SP 800-53 Revision 5 (System and Communications Protection family), NIST Cybersecurity Framework 2.0, IRS Publication 1075, and other applicable federal and state regulatory requirements. For detailed data classification requirements, see the ETSS Data Classification Policy (400.1).

2. Applicability

This policy applies to all State of Rhode Island Executive Branch departments, including agencies, boards, and commissions, as well as their employees (permanent, non-permanent, full-time, and part-time), interns, consultants, contractors, vendors, and any entity with approved access to State information systems and data, whether operated or maintained by the State or on behalf of the State.

3. Definitions

The following terms are defined for the purposes of this policy. For additional cryptographic, network, and security terminology, refer to the ETSS Glossary of Terms, Acronyms, and Definitions.

Classified Data
Any data that is not public, including confidential, sensitive, and private data as defined in the ETSS Data Classification Policy (400.1). Classified data requires additional security controls such as encryption and access restrictions. Examples include PII, PHI, FTI, PCI data, SSA data, and security-related system data.

Cryptographic Protection
The use of FIPS 140-2 or FIPS 140-3 validated encryption modules, algorithms, and protocols to

protect the confidentiality and integrity of data during transmission and at rest.

Boundary Protection
Controls implemented at information system perimeters and critical internal managed interfaces to monitor, control, and protect communications between trusted and untrusted networks.

4. Procedures for Compliance

The following requirements establish the system and communications protection controls that agencies and ETSS must implement. Security controls are assigned based on the Information Assurance Level (IAL) of the information system, aligned to the NIST SP 800-53 Rev. 5 Moderate baseline.

4.1 System and Communications Protection Policy and Procedures (SC-1)
Applies to: All systems (IAL1, IAL2)
Each agency shall develop, document, and disseminate a system and communications protection policy and supporting procedures. The ETSS CISO is designated as the official responsible for the enterprise policy. The policy shall be reviewed at least every three (3) years and following significant changes.

4.2 Separation of System and User Functionality (SC-2)
Applies to: Moderate and above (IAL2)
Information systems shall separate user functionality from system management functionality. Each agency shall: (a) implement ETSS-approved network segmentation mechanisms to separate application and database servers from the general network; (b) segregate production environments from testing, development, and other non-production environments; and (c) segregate wireless networks providing internal access from wireless networks providing unauthenticated or guest access.

4.3 Information in Shared System Resources (SC-4)
Applies to: Moderate and above (IAL2)
Information systems shall prevent unauthorized and unintended transfer of information via shared system resources, ensuring that information from prior users, roles, or processes is not available to subsequent users when shared resources are released back to the system.

4.4 Denial-of-Service Protection (SC-5)
Applies to: All systems (IAL1, IAL2)
Each agency shall protect information systems and network resources against denial-of-service attacks by employing boundary protection controls (firewalls, web application firewalls, intrusion detection/prevention systems, deny-all/permit-by-exception policies), periodic scanning, infrastructure redundancy, and DNS security measures.

4.5 Boundary Protection (SC-7)
Applies to: All systems (IAL1, IAL2)
The internal network shall be monitored, secured, and protected from untrusted external networks. Each agency shall:
a. Monitor, control, and protect communications at external boundary managed interfaces and at critical internal managed interfaces.
b. Implement subnetworks, such as demilitarized zones (DMZ), for publicly accessible system components that are physically and logically separated from internal networks.
c. Connect to external networks only through managed interfaces consisting of boundary protection devices arranged in accordance with ETSS security architecture requirements.

4.5.1 Access Points (SC-7(3))

Applies to: Moderate and above (IAL2)

Each agency shall limit the number of external network connections to the information system to facilitate monitoring of inbound and outbound communications traffic.

4.5.2 External Telecommunications Services (SC-7(4))

Applies to: Moderate and above (IAL2)

Each agency shall implement a managed interface for each external telecommunication service, establish traffic flow policies, protect confidentiality and integrity of transmitted information, document traffic flow exceptions with supporting business justification, review exceptions annually, and prevent unauthorized exchange of control plane traffic with external networks.

4.5.3 Deny by Default / Allow by Exception (SC-7(5))

Applies to: Moderate and above (IAL2)

Each agency shall employ a deny-all/allow-by-exception policy that denies network communications traffic by default and allows traffic by exception at managed internal and external interfaces for systems that process, store, receive, or transmit classified information.

4.5.4 Split Tunneling for Remote Devices (SC-7(7))

Applies to: Moderate and above (IAL2)

Information systems shall prevent remote devices from establishing a remote connection to the State network while simultaneously communicating via another connection to an external network (split tunneling). Remote connections shall utilize the ETSS VPN, which prevents split tunneling unless authorized and approved by the ETSS CISO. Approved exceptions for cloud service direct-connect circuits shall maintain endpoint monitoring, agent reporting, and conditional access policy enforcement.

4.5.5 Route Traffic to Authenticated Proxy Servers (SC-7(8))

Applies to: Moderate and above (IAL2)

Each agency shall route outbound web traffic from internal networks through authenticated proxy servers at managed interfaces to enforce content filtering, malware inspection, and access logging. Direct outbound internet access that bypasses proxy inspection is prohibited.

4.5.6 Host-Based Protection (SC-7(12))

Applies to: Moderate and above (IAL2)

Each agency shall deploy host-based protection tools on all managed endpoints and servers, including host intrusion prevention, host intrusion detection, or at minimum a host-based firewall, to provide an additional layer of boundary protection at the individual system component level.

4.5.7 Fail Secure (SC-7(18))

Applies to: Moderate and above (IAL2)

Boundary protection devices shall be configured to fail in a secure state in the event of an operational failure, preventing unauthorized traffic from passing through the boundary while the device is in a failed condition.

4.6 Transmission Confidentiality and Integrity (SC-8)

Applies to: Moderate and above (IAL2)

Each agency shall protect the confidentiality and integrity of transmitted classified data to both internal and external networks. Classified data transmitted on public networks shall be encrypted

using strong security protocols. Unencrypted transmission of classified data is prohibited. Email communications containing classified information shall be protected using enterprise email encryption capabilities.

4.6.1 Cryptographic Protection for Transmission (SC-8(1))

Applies to: All systems (IAL1, IAL2)

Each agency shall implement FIPS 140-2, FIPS 140-3 validated, or similar cryptographic mechanisms to prevent unauthorized disclosure and modification of information during transmission, including:

a. IPsec with AES-256 and SHA-256 or stronger to protect VPN traffic confidentiality and integrity.

b. TLS 1.2 or higher with approved cipher suites employing AES-256 to protect web traffic. Use of deprecated protocols (SSLv2, SSLv3, TLS 1.0, TLS 1.1) is prohibited. Valid signed TLS certificates from trusted providers are required for publicly accessible State websites and applications.

c. SFTP to protect data files transmitted over public or internal networks. Use of insecure FTP for non-public data is prohibited on public networks.

d. WPA2 Enterprise or stronger to protect data transmitted over the State wireless network.

4.7 Network Disconnect (SC-10)

Applies to: Moderate and above (IAL2)

Information systems shall automatically terminate network connections at the end of sessions, after no more than thirty (30) minutes of inactivity, and after an absolute time limit of twenty-four (24) hours. Sessions requiring more than twenty-four hours of unterminated connectivity must be documented in the System Security Plan and formally approved by the ETSS CISO via the ETSS Risk Acceptance process.

4.8 Cryptographic Key Establishment and Management (SC-12)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Establish and manage cryptographic keys using FIPS 140-2, FIPS 140-3 validated, or similar encryption modules.

b. Manage cryptographic keys within enterprise key management systems. Keys shall be protected from unauthorized modification, destruction, replacement, and disclosure. Private keys shall be kept confidential and protected with strong authentication.

c. Verify every three (3) years that encryption modules currently in use remain FIPS validated or adhere to accepted similar equivalent.

d. Replace cryptographic keys at end of life, when integrity may be compromised, or when the key has been compromised. Compromised keys shall be immediately revoked.

e. Notify the AIM, TSM, and system owner when a cryptographic key is lost or compromised.

f. Authenticate endpoints prior to exchanging or generating session keys using industry-approved cryptographic protocols (such as RSA, Diffie-Hellman, IKE, or ECDH).

4.9 Cryptographic Protection (SC-13)

Applies to: All systems (IAL1, IAL2)

Each agency shall implement FIPS 140-2, FIPS 140-3 validated, or similar cryptographic protections for classified data. ETSS-approved mechanisms include:

a. Symmetric encryption algorithms with 256-bit minimum key lengths (AES recommended).

b. Asymmetric encryption algorithms with 2048-bit minimum key lengths (RSA recommended);

Elliptic Curve Cryptography with 224-bit minimum key lengths.
c. Cryptographic hash functions using SHA-256 or stronger. Use of SHA-1 is prohibited unless formally authorized by the ETSS CISO.
State-owned laptops shall be encrypted with full-disk encryption prior to deployment. State-owned mobile devices and portable media containing classified data shall be encrypted using an appropriate method. Exceptions require formal CISO approval via the ETSS Risk Acceptance process.

4.10 Collaborative Computing Devices and Applications (SC-15)

Applies to: All systems (IAL1, IAL2)

Information systems shall prohibit remote activation of collaborative computing devices and provide explicit indication to physically present users when devices are active. Collaborative computing devices shall be disabled or disconnected from the network until ready for use.

4.11 Public Key Infrastructure Certificates (SC-17)

Applies to: Moderate and above (IAL2)

Each agency shall issue public key certificates in accordance with ETSS policies. State-owned websites and publicly accessible systems require certificates from a recognized certificate authority. Only approved trust anchors shall be included in trust stores managed by the agency.

4.12 Mobile Code (SC-18)

Applies to: Moderate and above (IAL2)

Each agency shall define acceptable and unacceptable mobile code, authorize, monitor, and control the use of mobile code within information systems. High-risk mobile code shall be obtained from trusted sources and signed with ETSS-approved certificates. Unsigned mobile code that requires access to local system or network resources is prohibited.

4.13 Secure Name/Address Resolution Service (SC-20, SC-21, SC-22)

Applies to: All systems (IAL1, IAL2)

Each agency shall ensure that: (a) authoritative DNS servers provide data origin authentication and integrity verification; (b) recursive/caching resolvers perform data origin authentication and integrity verification on responses; recursive lookups are disabled on publicly accessible DNS servers and zone transfers are restricted; and (c) name/address resolution services are fault-tolerant, load-balanced with at least two authoritative DNS servers in separate facilities, with internal and external DNS roles separated.

4.14 Session Authenticity (SC-23)

Applies to: Moderate and above (IAL2)

Information systems shall protect the authenticity of communications sessions using cryptographically secure session tokens transmitted over TLS-encrypted connections. Session identifiers shall expire or be invalidated upon session expiration or logout.

4.15 Protection of Information at Rest (SC-28)

Applies to: Moderate and above (IAL2)

Each agency shall protect the confidentiality and integrity of classified data at rest within information systems, virtual machines, endpoints, mobile devices, and removable media using FIPS 140-2, FIPS 140-3 validated, or similar cryptographic mechanisms with AES-256 encryption. Encryption keys shall be managed through enterprise key management systems where technically applicable.

4.15.1 Cryptographic Protection for Information at Rest (SC-28(1))

Applies to: Moderate and above (IAL2)

Each agency shall implement cryptographic mechanisms to prevent unauthorized

disclosure and modification of classified data at rest on all ETSS-managed assets or assets managed on behalf of ETSS. Encryption methods shall be appropriate for the device and location of the data, including full-disk encryption for laptops, device-level or container-level encryption for mobile devices, and encryption for portable storage media. Detailed encryption method guidance for specific device types and scenarios is documented in the ETSS Data Encryption Standard.

4.16 Process Isolation (SC-39)

Applies to: All systems (IAL1, IAL2)

Information systems shall maintain a separate execution domain for each executing process, assigning each process a distinct address space to manage inter-process communications and prevent one process from modifying the executing code of another.

4.17 System Time Synchronization (SC-45)

Applies to: Moderate and above (IAL2)

Each agency shall synchronize system clocks within information systems to an authoritative source of time to support accurate audit log timestamps, certificate validation, and time-dependent security functions.

5. Repercussions for Non-Compliance

Failure to comply with this policy may result in corrective action proportional to the severity of the violation. Consequences may include, but are not limited to:

a. Revocation of system or network access for unauthorized transmission of classified data.

b. Mandatory remediation of cryptographic or boundary protection deficiencies within defined timelines.

c. Formal counseling or written reprimand.

d. Referral to agency management for disciplinary proceedings.

e. Denial of system authorization for systems that do not meet encryption or boundary protection requirements.

f. Referral to law enforcement if unauthorized data exfiltration or deliberate circumvention of cryptographic protections is suspected.

Non-compliance findings shall be documented and tracked through ETSS governance processes and may be recorded in the agency Plan of Action and Milestones (POAM).

6. Roles and Responsibilities

The following roles are accountable for the implementation, monitoring, and enforcement of this policy:

Chief Information Security Officer (CISO)

Designated as the official responsible for the enterprise System and Communications Protection policy. Approves exceptions for deprecated protocols, split tunneling, and non-standard encryption. Oversees cryptographic standards compliance, boundary protection architecture, and FIPS validation verification.

ETSS Network Team

Responsible for implementing and managing boundary protection devices, firewall policies, VPN infrastructure, proxy server configurations, DNS architecture, and network segmentation. Manages traffic flow policies and control plane traffic protection at external telecommunications interfaces.

ETSS Infrastructure and Operations (I&O)

Responsible for enterprise cryptographic key management, full-disk encryption deployment, certificate

issuance and management, and implementation of encryption-at-rest controls across enterprise platforms and cloud services.

ETSS Security Operations

Responsible for monitoring boundary protection devices, detecting unauthorized communications, and coordinating incident response for communications security events.

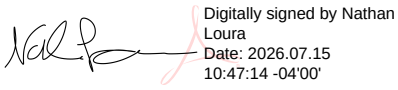
System Owners

Responsible for ensuring system and communications protection controls are implemented for their systems, including encryption of classified data in transit and at rest, session management, input validation, and mobile code restrictions.

Agency Information Managers (AIMs) / Technical Support Managers (TSMs)

Coordinate system and communications protection activities at the agency level. Receive notification of compromised cryptographic keys. Ensure agency compliance with encryption and boundary protection requirements.

7. Approval / Review Signatures



Chief Information Security Officer (CISO)
Division of Enterprise Technology Strategy and Services

Chief Digital Officer (CDO)
Division of Enterprise Technology Strategy and Services