**IT System and Communications Encryption Policy Template**

# PURPOSE

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure that “YOUR AGENCY NAME” develops, disseminates, and updates the IT System and Communications Encryption Policy. This policy and procedure establishes the minimum requirements for the IT System and Communications Encryption Policy.

This policy is intended to meet the control requirements outlined in SEC501, Section 8.16 IT System and Communications Encryption Family, controls SC-8, SC-9, SC-13, SC-17, SC-23, and SC-28 as well as additional Commonwealth of Virginia controls.

# SCOPE

All “YOUR AGENCY NAME” employees (classified, hourly, or business partners) as well as all sensitive “YOUR AGENCY NAME” systems

# ACRONYMS

CIO: Chief Information Officer

COV: Commonwealth of Virginia

CSRM: Commonwealth Security and Risk Management

DMZ: Demilitarized Zone

ISO: Information Security Officer

IT: Information Technology

ITRM: Information Technology Resource Management

SEC501: Information Security Standard 501

TIC: Trusted Internet Connection

“YOUR AGENCY NAME”: “YOUR AGENCY NAME”

VPN: Virtual Private Network

# DEFINITIONS

[See COV ITRM Glossary](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/EA_PSG_update_011510/ITRMGlossary_011510.pdf)

# BACKGROUND

The IT System and Communications Encryption Policy at “YOUR AGENCY NAME” is intended to facilitate the effective implementation of the processes necessary meet the IT system and communications encryption requirements as stipulated by the COV ITRM Security Standard SEC501 and security best practices. This policy directs that “YOUR AGENCY NAME” meet these requirements for all sensitive IT systems.

# ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibilities as described in the Statement of Policy section. The following Roles and Responsibility Matrix describe 4 activities:

1. Responsible (R) – Person working on activity
2. Accountable (A) – Person with decision authority and one who delegates the work
3. Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
4. Informed (I) – Person who needs to know of decision or action

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Roles** | Data Owner | System Owner | System Admin/Developer | Information Security Officer |
| **Tasks** |   |   |   |   |
| Configure information system to protect the integrity of transmitted information | R | A | R | R |
| Configure information system to protect the confidentiality of transmitted information | R | A | R | R |
| Configure wireless communications to utilize a encryption algorithm |  |  | R | A |
| Manage cryptographic keys |  | R | R | A |
| Generate encryption keys through an approved package |  | A | R | R |
| Secure private keys in motion or at rest |  | A | R | R |
| Implement required cryptographic protections |  | A | R | R |
| Define and document the selection and deployment of encryption technologies |  |  |  | A/R |
| Document appropriate encryption processes |  |  |  | A/R |
| Employ encryption over non-cov networks |  | A | R | R |
| Use data classification process to finalize application development processes |  |  |  | A/R |
| Include the proper use of encryption in training program |  |  |  | A/R |
| Follow policy to issue public key certificates |  | A | R | R |
| Select and implement protection mechanisms |  | A | R | R |
| Protect the confidentiality and integrity of information at rest | A |  | R | R |

# STATEMENT OF POLICY

In accordance with SEC501, SC-8, SC-9, SC-13, SC-17, SC-23, and SC-28, “YOUR AGENCY NAME” shall establish the minimum requirements for the encryption of sensitive data at rest or in motion, as well as encryption key management, and general encryption related controls. All newly implemented configurations must be Federal Information Processing Standard (FIPS) PUB 140-2 Level 1 compliant.

1. **TRANSMISSION INTEGRITY**
	1. The ISO or designee shall enforce the following requirements:

Note: This control applies to communications across internal and external networks.

* + 1. The information system must be configured to protect the integrity of transmitted information.
		2. If commodity commercial transmission services rather than a fully dedicated transmission service are used and it is infeasible or impractical to obtain from the service provider the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, then one or both of the following must be complied with:
			1. Appropriate compensating security controls must be implemented.
			2. The additional risk must be explicitly accepted.
		3. The following types of transmission require enhanced protection (e.g., cryptographic mechanisms) when integrity is an important consideration:
			1. Internal traffic within the information system and applications
			2. Internal traffic between two or more “YOUR AGENCY NAME” information systems
			3. External traffic to or across the Internet
			4. Remote access mechanisms (e.g., VPN, RAS, RDP)
			5. Email
			6. FTP transmissions
			7. Audio and video
			8. Wireless client to host communications
			9. Transmission of authentication data
			10. Transmission of data outside of the data’s broadcast domain.
		4. All communications that transfer confidentially sensitive data between web clients and web servers must employ the most current secure transport protocol that includes:
			1. Secure Sockets Layer (SSL) version 3.0
			2. Transport Layer Security (TLS)
		5. Instant messaging technologies, where allowed, must not be used to transmit any type of confidentially sensitive data.
		6. Cryptographic mechanisms must be employed to ensure changes to information during transmission are recognized, unless the transmission is protected by alternative physical measures (e.g., protective distribution systems).
		7. Encryption or digital signatures must be employed for the transmission of email and attached data that is sensitive relative to integrity*.*
1. **TRANSMISSION CONFIDENTIALITY**

Note: This control applies to communications across internal and external networks.

* 1. The ISO or designee shall enforce the following requirements:
		1. The information system must be configured to protect the confidentiality of transmitted information.
		2. Information of a confidentially sensitive nature (e.g., sensitive PII, trade secret information, confidentially sensitive business information, etc.) must be adequately protected from unauthorized disclosure at rest and in transit and must not be transmitted unprotected (e.g., not visible as clear text) over unsecured networks (e.g., the Internet).
		3. If commodity commercial transmission services rather than a fully dedicated transmission service are used and it is infeasible or impractical to obtain from the service provider the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, then one or both of the following must be complied with:
			1. Appropriate compensating security controls must be implemented.
			2. The additional risk must be explicitly accepted.
		4. The following types of transmission require enhanced protection (e.g., cryptographic mechanisms) when confidentiality is an important consideration:
			1. Internal traffic within the information system and applications
			2. Internal traffic between two or more “YOUR AGENCY NAME” information systems
			3. External traffic to or across the Internet
			4. Remote access mechanisms (e.g., VPN, RAS, RDP)
			5. Email
			6. FTP transmissions
			7. Web services
			8. Audio and video
			9. Wireless client to host communications
			10. Transmission of authentication data
			11. Transmission of data outside of the data’s broadcast domain.
		5. All communications that transfer confidentially sensitive data between web clients and web servers must employ the most current secure transport protocol which includes:
			1. SSL version 3.0 or higher where required for communication with the public
			2. TLS
		6. Instant messaging must not be used to transmit any type of confidentially sensitive data.
		7. Cryptographic mechanisms must be employed to prevent unauthorized disclosure of information during transmission, unless the transmission is protected by alternative physical measures.
		8. All wireless LAN and wireless bridge communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provide support for secure encryption protocols.
			1. Example: the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher.
		9. Encryption must be employed for the transmission of email and attached data that is sensitive relative to confidentiality.
			1. The issue of agency emails being intercepted, incorrectly addressed, or infected with a virus must be considered and planned.
1. **CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**
	1. The ISO or designee shall enforce the following requirements:
		1. Cryptographic keys must be established and managed by using manual procedures or automated mechanisms with supporting manual procedures, when cryptographic protection is required and the information system is not covered by an enterprise solution.
			1. A fully automated key management system is preferred to eliminate or reduce the opportunity for an individual to expose a key or influence the key creation.
			2. The secure key management system will be used for the administration and distribution of encryption keys.
		2. Availability of information must be maintained in the event of the loss of cryptographic keys by users.
		3. All encryption keys must be generated through an agency approved encryption package.
		4. Private Keys must be transmitted securely and encrypted at rest.
		5. If encryption keys are compromised, the Security Incident Response plan must be executed. If the key compromise leads to a data breach of public citizen information, the data breach notification process must be implemented immediately.
			1. Refer to the Guidance on Reporting Information Technology Security Incidents page on the “YOUR AGENCY NAME” Security Internet site.
			2. Refer to the IT Security Standard (SEC501) for Data Breach notification requirements.
2. **USE OF CRYPTOGRAPHY**
	1. The ISO or designee shall enforce the following requirements:
		1. The information system must implement required cryptographic protections using cryptographic modules that comply with applicable laws, directives, policies, regulations, standards, and guidance.
			1. All sensitive data must be encrypted with a validated technology solution defined in the National Institute of Standards and Technology FIPS PUB 140-2 document, Security Requirements for Cryptographic Modules. This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive information. The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. The minimum validated cryptographic technology solution that is adequate for “YOUR AGENCY NAME” encryption solutions is Level 1. The Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS PUB 140-2 which provides further guidance for selecting adequate encryption. This program and supporting documents may be found at the CMVP URL <http://www.nist.gov/cmvp>.
		2. Agency practices must be defined and documented for selecting and deploying encryption technologies and for the encryption of data.
		3. Before implementing encryption, appropriate processes must be documented. These processes must include the following components:
			1. Instructions in the IT Security Agency’s Incident Response Plan on how to respond when encryption keys are compromised;
			2. A secure key management system for the administration and distribution of encryption keys; and
			3. Requirements to generate all encryption keys through an approved encryption package and securely store the keys in the event of key loss due to unexpected circumstances.
		4. Encryption must be employed for the transmission of data that is sensitive relative to confidentiality or integrity over non-Commonwealth networks or any publicly accessible networks, or any transmission outside of the data’s broadcast domain. Digital signatures may be utilized for data that is sensitive solely relative to integrity.
		5. Application Development efforts must use the results of the Data Classification process against anticipated datasets to assess and finalize any encryption requirements.
			1. Data Classification guidance is provided in the IT Risk Management Guideline (SEC506), the “YOUR AGENCY NAME” IT Risk Assessment Policy and Procedure, and the “YOUR AGENCY NAME” IT System and Sensitivity Classification Policy and Procedure.
		6. The “YOUR AGENCY NAME” security awareness training program must include training for the proper use of encryption.
		7. The use of proprietary encryption algorithms is not permitted for the encryption of sensitive data under any conditions.
3. **PUBLIC KEY INFRASTRUCTURE CERTIFICATES**
	1. The ISO or designee shall enforce the following requirements:
		1. Public key certificates must be issued under a “YOUR AGENCY NAME”-defined certificate policy or obtained under an appropriate certificate policy from an approved service provider.
			1. “YOUR AGENCY NAME” shall provide oversight in the creation of Public Key Infrastructure (PKI) framework and services that provide the generation, production, distribution, control, revocation, recovery, and tracking of PKI certificates and their corresponding private keys.
			2. Public key certificates must be issued using a secure process that both verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.
4. **SESSION AUTHENTICITY**
	1. The ISO or designee shall enforce the following requirements:
		1. The information system must provide mechanisms to protect the authenticity of communications sessions.

Note: This control focuses on communications protection at the session versus packet level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the- middle attacks including session hijacking or insertion of false information into a session. This control is only implemented where deemed necessary by the organization (e.g., sessions in service-oriented architectures providing web-based services).

* 1. The System Owner shall select and implement protection mechanisms to ensure adequate protection of data integrity, confidentiality, and session authenticity in transmission;
		1. Mechanisms include but are not limited to the following:
			1. Security services based on IPsec
			2. VPNs
			3. TLS
			4. DNS
			5. SSH
			6. SSL
			7. Digital signatures
			8. Digital certificates
			9. Digital time stamping
			10. Approved encryption requirements and technology:
				1. FIPS 140-2
				2. Use of AES 128 bit or higher
1. **PROTECTION OF INFORMATION AT REST**
	1. The ISO or designee shall enforce the following requirements:

Note: This control is intended to address the confidentiality and integrity of information at rest in non-mobile devices and covers user information and system information.

* + 1. The information system must protect the confidentiality and integrity of information at rest (i.e., the state of information when it is located on a secondary storage device within an information system).
			1. User and system information at rest in non-mobile devices must be protected.
		2. The storage of sensitive data on any non-network storage device, excluding backup media, must be encrypted. A written exception approved by the Agency Head or his/her designee must be in place prior to storing encrypted sensitive data on non-network storage devices.
			1. Non-network storage devices include removable data storage media and the fixed disk drives of all desktops and mobile workstations, such as laptop and tablet computers, USB drives, CDs, etc.
		3. Sensitive data at rest must be encrypted when mandated by federal, state, or local laws as well as industry regulations, (e.g., IRS1075, HIPAA and PCI.)

Note: Configurations and/or rule sets for firewalls, gateways, intrusion detection/prevention systems, and filtering routers and authenticator content are examples of system information requiring protection. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate.

# ASSOCIATED

**PROCEDURE** “YOUR AGENCY NAME” Information Security Program

**AUTHORITY**

**REFERENCE** [*Code of Virginia, §2.2-2005 et seq.*](http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2005)

(Powers and duties of the Chief Information Officer “CIO”““YOUR AGENCY NAME””)

**OTHER**

**REFERENCE** [ITRM Information Security Policy (SEC519)](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Security_Policy_519_00_Final_0709.pdf)

 [ITRM Information Security Standard (SEC501)](http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501_06_07012011.pdf)

| Version History |
| --- |
| Version | Date | Change Summary  |
| 1 | 07/01/2014 | Supersedes “YOUR AGENCY NAME” CSRM Encryption Use Policy and “YOUR AGENCY NAME” CSRM Publicly Accessible Server Administration Procedure |
| 2 | 11/19/2021 | Formatting changes |