**IT System and Communications Protection 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 Protection Policy. This policy and procedure establishes the minimum requirements for the IT System and Communications Protection Policy.

This policy is intended to meet the control requirements outlined in SEC501, Section 8.16 IT System and Communications Protection Family, controls SC-1, SC-2, SC-3, SC-4, SC-7, SC-14, and SC-20 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

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

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 Protection Policy at “YOUR AGENCY NAME” is intended to facilitate the effective implementation of the processes necessary meet the IT system and communications protection 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** |   |   |   |   |
| Design and configure information system to separate user functionality from management functionality |  | A | R | R |
| Configure information system to isolate security functions from non-security functions |  | A | R | R |
| Configure information system to maintain a separate execution domain |  | A | R | R |
| Configure information system to prevent unauthorized and unintended information transfer via shared system resources |  | A | R | R |
| Configure information system to monitor and control communications |  | A | R | R |
| Protect the integrity and availability of publicly available information and applications. | A |  | R | R |
| Inventory publicly available servers |  |  | R | A |
| Log and save audit trails on sensitive systems | A |  | R | R |
| Perform security audits | A |  |  | R |
| Provide data origin and integrity artifacts with authoritative data. |  | A | R | R |

# STATEMENT OF POLICY

In accordance with SEC501, SC-1, SC-2, SC-3, SC-4, SC-7, SC-14, and SC-20, “YOUR AGENCY NAME” shall establish minimum requirements for the protection of systems and communications.

1. APPLICATION PARTITIONING
	1. The ISO or designee shall enforce the following requirements:
		1. The information system must be designed and configured to separate user functionality (including user interface services) from information system management functionality (e.g., functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access).

Note: An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different domain and with additional access controls.

* + 1. The information system must be designed and configured to either physically or logically separate user functionality from information system management functionality.
			1. Separation must be accomplished by using one of the following methods or a combination of methods, as applicable:
				1. Different computers
				2. Different partitions
				3. Different central processing units
				4. Different instances of the operating system
				5. Different network addresses
				6. Other methods as appropriate
		2. The following conditions must be met when designing, implementing, and managing web-based applications:
			1. Web content must be installed on a dedicated physical disk or logical partition that is separate from the storage locations for the operating system and web server application.
			2. A complete web content access matrix must be defined that identifies which folders and files within the web server’s document directories should be restricted and which should be accessible and by whom.
			3. Access to a specific web content file directory tree must be restricted by:
				1. Establishing related subdirectories exclusively for web server content files, including graphics but excluding scripts and other programs.
				2. Defining a single directory tree exclusively for all external scripts or programs executed as part of web content such as Common Gateway Interface (CGI), Active Server Pages (ASP), or PHP: Hypertext Preprocessor (PHP).
				3. Disabling the execution of scripts that are not exclusively under the control of administrative accounts by creating and controlling access to a separate directory intended to contain authorized scripts.
				4. Disabling the use of hard or symbolic links.
			4. The functionality of one process or service given to one application must not enable the same functionality for another application (e.g., access to a back-end database).
			5. A limit on hard drive space must be placed on resources dedicated for uploads from users to servers.
				1. Uploads must be placed on a separate partition to provide stronger assurance that the hard drive space limit cannot be exceeded.
			6. Log files must be stored in a location that is sized appropriately and must be stored on a separate partition or computer.
			7. On servers that use certificates, the original certificate must be stored in a folder or partition that is:
				1. Accessible by only authorized web or system administrators
				2. Secured by appropriate authentication mechanisms
			8. On servers that use certificates, a file integrity checker must be run on the server to monitor for any changes to the certificate.
		3. The information system must be configured to prevent users from performing any functions that are not explicitly authorized for their roles.
		4. Sensitive information shall not be stored in hidden fields that are part of the application interface.
1. SECURITY FUNCTION ISOLATION
	1. The ISO or designee shall enforce the following requirements:
		1. The information system must be configured to isolate security functions from non-security functions by means of isolation boundaries (implemented via partitions and domains) that control access to and protect the integrity of the hardware, software, and firmware that perform those security functions.
		2. The information system must be configured to maintain a separate execution domain (e.g., address space) for each executing process.
2. INFORMATION IN SHARED RESOURCES
	1. The ISO or designee shall enforce the following requirements:

Note: The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.

* + 1. The information system must be configured to prevent unauthorized and unintended information transfer via shared system resources.

Note: The control of information in shared resources is also referred to as object reuse.

* + 1. When configuring a host operating system, the following must be complied with:
			1. Temporary files created by the server application must be restricted to a specified and appropriately protected subdirectory, when possible.
			2. Access to any temporary files created by the server application must be limited to the service processes that created the files, when possible.
		2. Any previous information content of the information system must be made unavailable upon the allocation of the resource to all subjects, and this must be carried out through the implementation of safeguards, including but not limited to the following:
			1. Temporary pages must not be indexed.
		3. The information system object reuse features must be configured to delete information when no longer needed.
			1. Cookies placed onto users' systems must not contain sensitive data or Personally Identifiable Information (PII).
			2. The information system must overwrite sensitive data in memory after the use of the data.
				1. Sensitive information includes passwords, secret keys, session keys, private keys, or any other highly sensitive data such as PII or medical records.
			3. At the end of a session, the information system must delete all temporary files created during the session.
			4. Before shutdown, the application must delete or erase all temporary files, cache, data, and other objects it created during its execution.
			5. On a weekly basis, the information system must search and delete Word, Outlook, and Internet Explorer temporary files.
		4. The information system must not generate core dumps when the information system fails.
		5. Information on backup and storage media (e.g., memory, disk drives, removable media including tapes, flash drives, optical disks) must be protected as follows:
			1. The media must be cleared and purged before reuse or before using for other purposes by using Agency-approved and validated overwriting technologies/methods/tools.
			2. The media must be destroyed by using Agency-approved and validated technologies/methods/tools.
		6. Printers and copiers must be configured to not recall data from memory or disks after printing processes.

Note: This control does not address: (i) information remanence which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the information system for which there is only a single user/role.

1. BOUNDARY PROTECTION
	1. The ISO or designee shall enforce the following requirements:
		1. The information system must be configured to monitor and control communications:
			1. At the external boundary of the system
			2. At key internal boundaries within the system
		2. The information system must connect only to external networks or information systems, through managed interfaces approved by “YOUR AGENCY NAME”.
			1. These managed interfaces must consist of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in accordance with an effective, security architecture.
				1. For example, the architecture may consist of firewalls protecting routers and application gateways residing on a protected sub-network commonly referred to as a demilitarized zone or DMZ.
			2. Connections must be consistent with “YOUR AGENCY NAME”’s enterprise technology and security architecture.
		3. “YOUR AGENCY NAME” shall consider the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services.
			1. When commercial telecommunications services are employed, either 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.

Note: Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions.

* + 1. Boundary/edge devices (e.g., firewalls, routers) must be configured to protect and control access to Agency information resources.
			1. Incoming network traffic must be inspected and requests that do not comply with applicable policy must be denied.
			2. External web traffic must be restricted only to organizational web servers within managed interfaces.
			3. Traffic from outside a designated boundary that claims to be from within the designated boundary must be blocked.
				1. This applies to any traffic from the external network that has a source address that should reside on the internal network.
			4. Web requests that are not from an authorized internal web proxy must not be passed to the Internet.
		2. Information systems must detect and block unauthorized scanning activity that originates outside of its network, within its network, and between information systems.
		3. The following must be complied with when securing network device management technologies/tools:
			1. There must be sufficient capacity to collect, store, and view system logging information from all critical Agency infrastructure devices.
			2. Data and alerts from specialized applications (e.g., IDS/IPS) must be logged to separate management hosts that are better equipped to handle time-critical alarms.
			3. To ensure that log messages are time-synchronized to each other, clocks on hosts and network devices must be synchronized using Network Time Protocol (NTP) or other approved services.
			4. Management channels that need to be active at all times, such as Simple Network Management Protocol (SNMP), must be used with utmost caution due to the inherent vulnerabilities.
				1. Where SNMP is in use, access to devices must be read-only.
		4. The following must be complied with when securing routers:
			1. Router configurations and associated documentation must be treated as confidentially sensitive information and must be available to only authorized personnel (e.g., authorized administrators, auditors, security oversight personnel).
			2. All forms of router access, including SNMP and Hypertext Transfer Protocol (HTTP), must be restricted in accordance with the manufacturer’s recommendation.
			3. All passwords must be encrypted.
			4. Secure Shell (SSH) must be used to access a router interface in order to defeat packet sniffers.
				1. Telnet is prohibited from use.
			5. All routers must employ system use notification messages.
			6. Suitable forms of logging must be employed.
				1. Examples of logging are system logging; Authentication, Authorization, and Accounting (AAA); and SNMP trap logging.
			7. Internet Protocol (IP) routing must be secured with anti-spoofing, route advertisement authentication, and related measures.
			8. Unnecessary services such as finger, Cisco Discovery Protocol (CDP), File Transfer Protocol (FTP), and Trivial File Transfer Protocol (TFTP) must be disabled.
			9. Router software (i.e., operating system) must be kept up-to-date and patches must be applied.
		5. The following must be complied with when securing network switches:
			1. Procedures for carrying out change control and configuration analysis must be in place for switches.
			2. Unused switch ports must be disabled to prevent hackers from connecting to unused ports and communicating with the rest of the network.
			3. For ports that require trunking, a dedicated Virtual Local Area Network (VLAN) identifier must be used.
			4. Switches must be configured in high-security mode to defeat Address Resolution Protocol (ARP) spoofing and ARP poisoning attacks.
			5. Switches must be configured to send all traffic to network-based IDS/IPS on the public web server network segment or to other network segments guarded by an IDPS.
		6. The following must be complied with when securing networked hosts:
			1. Unused or unneeded services and applications on hosts must be disabled.
			2. All remote access to hosts must occur over secure channels.
				1. Secure channels include encrypted network connections using SSH or Internet Protocol Security (IPsec).
			3. Network connections must be configured to prevent removal or relocation of a host except by authorized personnel and in conformance with configuration management and change control processes.
			4. All networked hosts must be scanned for viruses.
			5. At a minimum, IDS/IPS technology must be deployed for hosts that use end-to- end encrypted communications.
		7. The following must be complied with when securing IDS/IPS:
			1. Network Intrusion Detection System (NIDS) and/or Host Intrusion Detection System (HIDS) must be used as appropriate for the protection of agency assets.
			2. The IDS/IPS engines must be tuned and maintained by security personnel to maximize effectiveness of detection and minimize the occurrence of false positives and false negatives.
			3. IDS/IPS databases must be continuously updated with the latest attack signature information.
			4. Outsourced solutions must be carefully evaluated to ensure that agency security and performance requirements are met.
		8. The following must be complied with regarding firewall management:
			1. Firewall configurations and associated documentation must be treated as confidentially sensitive information and must be available to only authorized personnel (e.g., authorized administrators, auditors, security oversight personnel).
			2. An effective set of procedures must be in place to distribute firewall update bulletins and security patches.
			3. Firewall patches must be installed as soon as possible after the respective vendors release them and the patches are tested.
			4. Unneeded services (e.g., telnet) must be disabled on the firewall.
			5. The firewall must have at least two network interfaces (i.e., dual-homed), one for the private network it is intended to protect and one for the external network to which it is exposed.
			6. The following testing must be performed on an annual basis on firewalls and management consoles:
				1. Penetration testing against the firewall
				2. Verification that the firewall is properly configured and patched and validation that the firewall is operating as intended.
			7. Firewall security procedures must be reviewed on a regular basis by the ISO or delegate.
		9. Publicly accessible information system components (e.g., public web servers) must be physically allocated to separate sub-networks with separate, physical network interfaces.
		10. Public access into the organization’s internal networks must be prevented by the information system except as appropriately mediated by managed interfaces employing boundary protection devices.
		11. The number of access points to the information system must be limited to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.

Note: The TIC initiative is an example of limiting the number of managed network access points.

* + 1. A managed interface must be implemented for each external telecommunication service.
			1. Security controls must be employed as needed to protect the confidentiality and integrity of the information being transmitted.
		2. A traffic flow policy must be established for each managed interface.
			1. Each exception to the traffic flow policy must be documented with a supporting mission/business need and the duration of that need.
			2. Exceptions to the traffic flow policy must be reviewed at least once every 60 days.
			3. Traffic flow policy exceptions that are no longer supported by an explicit mission/business need must be removed.
		3. The information system must be configured at managed interfaces to deny network traffic by default and allow network traffic by exception (i.e., deny all, permit by exception).
		4. The information system must be configured to prevent remote devices (e.g., notebooks/laptop computers) that have established a non-remote (e.g., VPN) connection with the system from communicating outside of that communications path with resources in external networks.
			1. Remote devices must be configured via settings that are not configurable by the user of that device to prevent “split tunneling”.

Note: Split tunneling might otherwise be used by remote users to communicate with the information system as an extension of that system and to communicate with local resources such as a printer or file server. Since the remote device, when connected by a non-remote connection, becomes an extension of the information system, allowing dual communication paths such as split tunneling would be, in effect, allowing unauthorized external connections into the system.

* + 1. The unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary must be prevented when there is an operational failure of the boundary protection mechanisms.
		2. The information system must be configured with host-based boundary protection mechanisms (e.g., host-based firewalls) for servers, workstations, and mobile devices.
1. PUBLIC ACCESS PROTECTIONS

Note: The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls.

* 1. The ISO or designee shall enforce the following requirements:
		1. The information system must protect the integrity and availability of publicly available information and applications.
		2. The information system architecture must be designed so that publicly available servers are hosted in a DMZ.
		3. The information system must be configured to enforce the following:
			1. Prevent unauthorized users from changing or deleting any established reference links, or associations, or other relationships between data elements.
			2. Restrict system-related data against modification by public users, unless that data is intended to be altered by the public.
			3. Prevent the modification of any data elements that are designated as read- only.
				1. The information system must also issue a warning reminder to the user that they are not authorized to move, change, or delete read-only data.
			4. Protect the browser or other client application session cookies from tampering.
			5. Protect user identity information stored on the browser or client platform from disclosure and tampering.
			6. Prevent users from accessing the file system directory indicated by a path name.
		4. Routine system updates must be performed on all publicly accessible system components to maintain appropriate and security-required patch levels.
		5. Scripts must be secured, reviewed, and tested against exploits that might allow direct access to the underlying operating system or other compromises of the application.
		6. Where the application promotes or permits public access, authorization must be obtained to ensure that only the appropriate types of information are made available to the public.
		7. All publicly accessible servers will be inventoried on a regular basis (minimally every 12 months) to ensure the ISO can certify existing services are not vulnerable to exploit.
		8. The ISO or designee will review all internal and external services prior to being developed or modified that rely on “YOUR AGENCY NAME”’s systems, servers, mainframes, networks, or the Internet (ref. “YOUR AGENCY NAME”\_ITIES\_Architectural Review (VAR) Policy and Procedure).
		9. All “YOUR AGENCY NAME” Internet accessible servers must be identified by the system administrator who is responsible for system administration. Server configurations must be established and maintained based on business needs by the system owner. The ISO will approve and monitor configuration compliance.
		10. System Owner must establish a process for updating the configurations, which includes review and approval by the ISO. The ISO establishes the security baseline configurations.
	2. The ISO or designee shall enforce the following security best practices to promote secure server administration:
		1. Operating System configuration should be in accordance with approved “YOUR AGENCY NAME” Commonwealth Security and Risk Management guidelines where appropriate.
		2. Services and applications that will not be used must be disabled where practical.
		3. Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
		4. The most recent security patches must be installed on the system as soon as practical and in accordance with applicable standards, the only exception being when immediate application would interfere with business requirements.
		5. Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
		6. Always use standard security principles of least required access to perform a function.
		7. Do not use a privileged account when a non-privileged account will do.
		8. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
		9. Administrative access should only be performed from a COV-managed device or otherwise approved system.
		10. Servers should be physically located in an access-controlled environment. Servers are specifically prohibited from operating from uncontrolled cubicle areas.
	3. The ISO or designee shall enforce the following security best practices to promote secure server monitoring:
		1. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
			1. All security related logs will be accessible for a minimum of 90 days.
			2. Daily incremental tape backups will be retained for at least 1 month.
			3. Weekly full tape backups of logs will be retained for at least 1 month.
			4. Monthly full backups will be retained for a minimum of 2 years.
			5. Security-related events will be reported to CSRM who will review logs and report incidents to IT management.
		2. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
			1. Port-scan attacks.
			2. Evidence of unauthorized access to privileged accounts.
			3. Anomalous occurrences that are not related to specific applications on the host.
	4. Security Audits will be performed on a regular basis by “YOUR AGENCY NAME”’s CSRM or other authorized organizations (e.g. Security Consultant). Audits will be managed by “YOUR AGENCY NAME”’s CSRM.
1. SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)
	1. The ISO or designee shall enforce the following requirements:
		1. The information system must provide additional data origin and integrity artifacts (e.g., digital signatures, cryptographic keys) along with the authoritative data (e.g., DNS resource records) the system returns in response to name/address resolution queries.
			1. This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service.
		2. A list must be maintained of the individuals authorized to administer each zone and name server.
			1. The list must indicate each zone and name server for which an individual has responsibility.
		3. The DNS server software must execute only on agency-approved and hardened operating systems.
		4. The information system’s DNS server software and related portions of the underlying operating system must be configured to guard against adverse attacks to circumvent the DNS.
			1. Mitigation actions must include the following:
				1. Configure the information system to ensure that hosts outside a boundary cannot directly query or request a zone transfer from a DNS that resides on the internal network (i.e., not in a DMZ).
				2. Disable dynamic updates unless the DNS software is configured to require that all dynamic updates be cryptographically authenticated.
				3. Review DNS logs daily or employ a near real-time log analysis or network management tool that immediately alerts an administrator of critical DNS system messages.
				4. Configure the DNS software to log, at a minimum, success and failure of the following events:

Start and stop of the name server service or daemon.

Zone transfers

Zone update notifications

Dynamic updates

* + - 1. Back up DNS configuration and resource record data daily.
		1. The aforementioned identified mechanisms must be re-evaluated on an annual basis to ensure that the mechanisms continue to meet the security needs of the information system.

# ASSOCIATED

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

**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 Firewall VPN Policy and “YOUR AGENCY NAME” CSRM Publicly Accessible Server Administration Policy |
| 2 | 11/22/2021 | Formatting changes |