**Remote and Wireless Access Controls 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 Remote and Wireless Access Controls Policy. This policy and procedure establishes the minimum requirements for the remote and wireless access controls.

This policy is intended to meet the control requirements outlined in SEC501, Section 8.2 Security Access Control Family, Controls AC-17, AC-17-COV, and AC-18, AC-18-COV.

# SCOPE

All “YOUR AGENCY NAME” employees (classified, hourly, or business partners) who require access to “YOUR AGENCY NAME”’s IT systems as well as all “YOUR AGENCY NAME” information and information systems including systems used or operated by contractors and other third parties on behalf of “YOUR AGENCY NAME”.

NOTE:

* + - 1. Public web servers or systems specifically designed for public access are not in scope to this policy.
			2. A Virtual Private Network (VPN) when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the agency establishes a network connection between organization controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network).

# ACRONYMS

AP: Access Point

CIO: Chief Information Officer

COV: Commonwealth of Virginia

CSRM: Commonwealth Security and Risk Management

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

ISO: Information Security Officer

IT: Information Technology

ITRM: Information Technology Resource Management

LAN: Local Area Network

SEC501: Information Security Standard 501

SSID: Service Set Identifier

“YOUR AGENCY NAME”: “YOUR AGENCY NAME”

VPN: Virtual Private Network

WLAN: Wireless Local Area Network

WPA-2: Wi-Fi Protected Access, version 2

# DEFINITIONS

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

# BACKGROUND

Remote and wireless access to IT systems and data exposes the COV to substantial risk and vulnerability. As such, proper controls are required to ensure that “YOUR AGENCY NAME” owned and operated systems are protected and that risk is mitigated to the greatest extent possible. This policy directs that “YOUR AGENCY NAME” meet the requirements as stipulated by COV ITRM Security Standard SEC501 and security best practices.

# 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** | User  | User Manager | System Owner | System/Network Admin | Information Security Officer |
| **Tasks** |   |   |   |   |   |
| Establish usage restrictions and implementation guidance for remote access |  |  | R | R | A |
| Authorizes execution of privileged commands and access to security-relevant information via remote access. |  |  | A | R | R |
| Authorizes the system for remote access. |  |  | A | R | R |
| Obtains explicit authorization for remote access. | I | A | R | R |  |
| Protect information about remote access mechanisms from unauthorized use and disclosure. | A |  | R | R |  |
| Configure remote access for users and systems in accordance to this policy. |  |  | A | R |  |
| Establishes usage restrictions and implementation guidance for wireless access. |  |  | R | R | A |
| Obtains explicit authorization for wireless access prior to using wireless access capabilities. | I | A | R | R |  |
| Authorizes wireless access to the information system. |  |  | A | R | R |
| Monitors remote access and wireless access for unauthorized access. |  |  | A | R |  |

# STATEMENT OF POLICY

This statement of policy covers, SEC501, AC-17 Remote Access and AC-18 Wireless Access, as well as, all related COV additions to those controls. Remote access and wireless access to “YOUR AGENCY NAME”’s IT systems and data is to be permitted only as necessary to support the purpose, goals of the agency and therefore each user’s authorized job functions. Enforcement of the restrictions outlined in this policy is accomplished by controls as implemented:

* “YOUR AGENCY NAME” Logical Access Control Policy
* “YOUR AGENCY NAME” IT Security Audit, Logging and Monitoring Policy
* “YOUR AGENCY NAME” Security Awareness and Training Policy
1. **REMOTE ACCESS**

Remote access is any access to an agency information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet or connection (e.g., dial-up, broadband, wireless).

* 1. “YOUR AGENCY NAME” shall or shall ensure the following requirements are met:
		1. The ISO or designee shall establish usage restrictions and implementation guidance for each allowed remote access method implemented by the agency.
			1. All remote access methods shall be implemented through a limited number of managed access control points.
		2. The System Owner shall authorize the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.
		3. The System Owner and/or Data Owner shall authorize whether the system is eligible for remote access and which methods of remote access are allowed for the system and data.
			1. The system owner will ensure that if only some portions of the system are available for remote access, the proper documentation is in place for how access control is checked for origination (remote vs. local) prior to granting the appropriate access level.
		4. The user must obtain explicit authorization for remote access prior to using remote access capabilities and only use their assigned unique user ID and password.
		5. Automated mechanisms shall be deployed to facilitate the monitoring and control of remote access methods that allow the agency to audit user activities on system components such as servers, workstations, notebook/laptop computers to ensure compliance with this policy.
			1. All remote access will be monitored and appropriate action is taken upon discovery of an unauthorized connection to the information system.
		6. Remote access to sensitive IT systems, data and file transfers must be protected by means of encryption to protect the confidentiality and integrity of remote access sessions. Encryption must begin with the initiation of the remote access session, include all user identification and authentication, and not end until the session is terminated.
		7. All users must protect information about remote access mechanisms from unauthorized use and disclosure.
		8. All remote sessions for accessing sensitive data or development environments must employ two-factor authentication and be audited.
			1. Additional security measures may be required above and beyond standard bulk or session layer encryption, such as Secure Shell (SSH), VPN with blocking mode enabled.
		9. All TCP and UDP ports except for explicitly identified components in support for specific operational requirements must be disabled.
		10. When connected to internal networks from “YOUR AGENCY NAME” guest networks or non-”YOUR AGENCY NAME” networks, data transmission shall only use full tunneling and not use split tunneling.
		11. Where supported by features of the system, session timeouts for remote access shall be implemented after a period of not longer than 30 minutes of inactivity or less. Where not supported by features of the system, mitigating controls must be implemented.
1. **WIRELESS ACCESS CONTROLS**

Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. In certain situations, wireless signals may radiate beyond the confines and control of agency controlled facilities.

* 1. “YOUR AGENCY NAME” shall or shall ensure the following requirements are met:
		1. The ISO or designee shall establish usage restrictions and implementation guidance for wireless access implemented by the agency.
		2. The System Owner and/or Data Owner shall authorize whether the system is eligible for wireless access and which methods of remote access are allowed for the system and data.
		3. The user must obtain explicit authorization for wireless access prior to using wireless access capabilities and only use their assigned unique user ID and password.
		4. Automated mechanisms shall be deployed to facilitate the monitoring and control of wireless access that allow the agency to audit user activities on system components such as servers, workstations, notebook/laptop computers to ensure compliance with this policy.
			1. All wireless access will be monitored and appropriate action is taken upon discovery of unauthorized connection to the information system.
		5. The following enhancements must be deployed for Sensitive Systems:
			1. The information system protects wireless access to the system using authentication and encryption. Authentication applies to user, device, or both as necessary;
			2. “YOUR AGENCY NAME” monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points, and take appropriate action if an unauthorized connection is discovered;
			3. “YOUR AGENCY NAME” will disable, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment;
			4. “YOUR AGENCY NAME” does not allow users to independently configure wireless networking capabilities, which include access points, authentication controllers, antennae, etc.; and
			5. “YOUR AGENCY NAME” does not allow users to create ad-hoc, peer-to-peer, or other unauthorized networks.
		6. The following requirements shall be met in the deployment, configuration and administration of WLAN infrastructure connected to any internal “YOUR AGENCY NAME” network:
			1. Client devices connecting to the WLAN must utilize two-factor authentication through the use of digital certificates;
			2. WLAN infrastructure must authenticate each client device prior to permitting access to the WLAN;
			3. LAN user authorization infrastructure (i.e., Active Directory) must be used to authorize access to LAN resources;
			4. Only “YOUR AGENCY NAME” owned or leased equipment shall be granted access to an internal WLAN;
			5. All WLAN 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 (i.e., the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher);
			6. Physical or logical separation between WLAN and wired LAN segments must exist;
			7. All “YOUR AGENCY NAME” WLAN access and traffic must be monitored for malicious activity, and associated event log files stored on a centralized storage device;
			8. Configuration and security data associated with the WLAN must not be provided to unauthorized devices. For example, SSID broadcasting will be disabled; and
			9. WLAN clients must be configured to only permit infrastructure mode communication.
		7. The following must be in place for wireless networks which will only provide unauthenticated access to the Internet:
			1. WLAN Hotspots must have logical or physical separation from the agency’s LAN;
			2. WLAN Hotspots must have packet filtering capabilities enabled to protect clients from malicious activity;
			3. WLAN Hotspot access and traffic must be monitored for malicious activity, and log files stored on a centralized storage device; and
			4. Where “YOUR AGENCY NAME” clients are concerned, WLAN clients will only permit infrastructure mode communication.
		8. The following network configuration must be in place when bridging two wired LANS:
			1. All 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 methods (i.e., the Courter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard Cipher);
			2. Wireless bridging devices will not have a default gateway configured;
			3. Wireless bridging devices must be physically or logically separated from other networks;
			4. Wireless bridge devices must only permit traffic destined to traverse the bridge and should not directly communicate with any other network;
			5. Configuration and security data associated with the WLAN must not be provided to unauthenticated devices. For example, SSID broadcasting will be disabled; and
			6. Wireless bridging devices must not be configured for any other service than bridging (i.e., a wireless access point).

# 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 | Original. Previous versions of “YOUR AGENCY NAME” CSRM Remote Access Policy and “YOUR AGENCY NAME” CSRM Wireless Procedure were updated to reflect ITRM Information Security Standard SEC501 Revision 8 and combined to form this new policy. |
| 2 | 12/16/2021 | Formatting changes |