Policy and Procedure 9-1
Information Security: Access Control

Issued By:	Robert W. Farrell, State Forester	DocuSigned by: Robert W. Farrell 2115C3D38FCF4E7... 7/9/2024
Effective Date:	July 01, 2024	
Codes/Mandates:	Code of Virginia §2.2-2005 Creation of Agency; appointment of Chief Information Officer Code of Virginia §2.2-2007 Powers of the CIO. Code of Virginia §2.2-2014 Submission of information technology plans by state agencies and public institutions of higher education; designation of technology resource. Code of Virginia §2.2-603(F) Authority of agency directors.	
References:	Commonwealth Information Technology Resource Management (ITRM) Information Security Policy SEC 519-00, ITRM Standard SEC530: Information Security Standard DHRM Policy 1.75 Use of Electronic Communications and Social Media Policy and Procedure 08-003 Human Resources Equal Opportunity and Employment Practices Policy and Procedure 09-007 Identification and Authentication Policy and Procedure 09-008 Information Security Incident Response	
Forms:	N/A	

CONTENTS

PURPOSE

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standard, to ensure that Virginia Department of Forestry develops, disseminates, and updates access controls to all DOF systems. This policy and procedure establishes the minimum requirements for the control of logical access to DOF's computer systems including test and production.

This policy is intended to meet the control requirements outlined in SEC530, Section 8.1 Access Control Family, Controls AC-1 through AC-22, to include specific requirements for COV.

SCOPE

The Virginia Department of Forestry is committed to the implementation of an effective information security program. This policy applies to all Department of Forestry employees (classified, hourly, or business partners) who administer computer systems owned and/or operated by Department of Forestry, data owners, as well as all system owners. This policy also includes virginia.gov or other contractually hosted Web sites or server administration.

Definitions and Acronyms

"Agency" and **"DOF"** means the Virginia Department of Forestry.

"Agency Information Technology Resource" and **"AITR"** means the agency employee who is designated by the state forester to be responsible for compliance with the policies, standards and guidelines established by the chief information officer for the Commonwealth, as required by Code of Virginia §2.2-2014(B). The director of information technology and helpdesk analyst currently serves in this role.

"Commonwealth" and **"COV"** means the Commonwealth of Virginia.

"Data owner" means the agency manager or supervisor, designated by the state forester, who defines, manages and controls the use of data and ensures compliance with adopted standards.

"Electronic files" means media content (other than computer programs or system files) that are intended to be used in either an electronic form or as printed output. This includes, but is not limited to, email, documents, spreadsheets, images, photographs, presentations, and GIS files.

"Information Security Officer" and **"ISO"** means the agency employee who is designated by the state forester to develop and manage the agency's information security program, as required in the Commonwealth's Information Security Standard, SEC530.

"Information technology resources" means any device or equipment that can be used to access and/or store electronic information including, but not limited to, laptops, desktops, tablets, mobile phones, thumb drives, external hard drives, and networked printers.

"SEC530" means the Commonwealth Information Security Standard 530

"System administrator" means the agency employee who implements, manages, and/or operates a system at the direction of the system owner or data owner.

"System owner" means the agency manager or supervisor who is responsible for the operation and oversight of any given agency business system.

ACRONYMS

AC:	Access Control
AP:	Access Point
CIO:	Chief Information Officer
COV:	Commonwealth of Virginia
CSRM:	Commonwealth Security and Risk Management
DHRM:	Department Human Resource Management
DOF:	Department of Forestry
IDS:	Intrusion Detection System
IPS:	Intrusion Prevention System
ISO:	Information Security Officer
IT:	Information Technology
ITRM:	Information Technology Resource Management
LAN:	Local Area Network
SEC530:	Information Security Standard 530
SSID:	Service Set Identifier
SSP:	System Security Plan
VITA:	Virginia Information Technology Agency
VPN:	Virtual Private Network
WLAN:	Wireless Local Area Network
WPA-2:	Wi-Fi Protected Access, version 2 "AC" means access control.

BACKGROUND

Managing access control of a system is one the most important steps in ensuring the security of the system. As such Department of Forestry systems require a well-defined and well-implemented set of access controls. This policy directs systems owned and/or operated by the Department of Forestry meet these requirements as stipulated by COV ITRM Security Standard SEC530 and security best practices.

ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibility as described in the Statement of Process section. The following Roles and Responsibility Matrix describes 4 role specific activities:

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

Tasks	Users	User Supervisor	System Owner	System Admin	Human Resource Manager	Information Security Officer
Create an access control document.			C	C		A/C/R
Review accounts and privileges on an annual basis.	I	R				A/I
Approve all user logical access to system.		R		C/R		
Ensure that no local administrator rights are granted.				C/R		A/R
Notify system owner to remove an account or change access.		A		I/R	A	
Disable or change user's access.		I/A		I/R	A	
Monitor account usage.				A/R		
Approve emergency access.	I		A	R		I
Keep all user account data and information on file.			A/R	C		
Ensure that at least two individuals have administrative accounts to each IT system.			A	R		
Ensure that system administrators have both an administrative account and a user account.			A	R		
Deactivate temporary accounts.			A	R		
Verify that background checks have been completed before establishing accounts				I	A/R	
Ensure that users are not sharing accounts.	A	A/R				
Ensure that access credentials are delivered in a confidential manner.	I			R/A		
Audit account creation, modification, disabling, and termination actions.				R		R/A
Associate access levels with group membership.				A/R		
Prohibit guest accounts on sensitive systems.				A/R		
Document all hardware and service accounts.				A/R		
Document where two-factor authentication cannot be used.				A/R		I
Investigate any unusual system access activities.				A/R		I
Employ and document access control mechanisms.				A/R		I
Control information flow.				A/R		
Implement and document separation of duties.				A/R		I
Ensure the concept of least privilege for each user.				A/R		
Implement a policy for unsuccessful logins.				A/R		I
Display an approved system notification message.	I			A/R		
Implement a session locking policy.				A/R		
Identify and document user actions that can be performed without identification and authentication.				A/R		

Designate and train individuals authorized to post information on a publicly accessible system.			A	R		I
Review content of publicly accessible information.			A	R		I
Remove nonpublic information from publicly accessible systems, if discovered.			A	R		I

STATEMENT OF POLICY

In accordance with SEC530, AC-1 through AC-14, and AC-22, Access Control, Department of Forestry will develop, disseminate, and review/update the Information Security: Access Controls Policy and Procedure on an annual basis.

Logical Access

Account Management (AC-2)

1. All supervisors will ensure proper access management to agency-owned systems and systems belonging to business partners who house DOF-owned information.
2. The ISO shall create an Access Control document that defines the processes and procedure that the organization will use to manage access to DOF systems. The document will include, at a minimum, the following:
    a. An account type dictionary which includes a list of all account types used by the organization / system (i.e., individual, group, system, application, guest/anonymous, temporary, etc.) and a definition of that account type.
    b. A group membership policy definition section which establishes a list of all groups and conditions for group membership. For example, group membership includes but is not limited to accesses grouped by Read Only, Read/Write.
    c. A well-defined process for identifying authorized users access to the information system and specifying access privileges. The process will include:
        i. Definition of appropriate approvals required for requests to establish new accounts.
        ii. Definition of appropriate approvals required for requesting modification (addition or subtraction of privileges).
        iii. Process for establishing, activating, modifying, disabling, and removing accounts.
        iv. Procedures for specifically authorizing and monitoring the use of guest/anonymous and temporary accounts.
3. The supervisor shall review accounts and privileges at least on an annual basis and report this information to the ISO.
4. The user's supervisor and the system administrator shall approve all user logical access to DOF systems.
    a. As part of the access request, the user's supervisor must include the user's need for access.
    b. The System Administrator maintains the documented approvals.
    c. The ISO shall approve accounts for users requiring administrative and/or privileged access.
5. The ISO and the System Administrator will ensure that no local administrator rights are granted:
    a. Unless there is a documented exception on file, for employees that are primarily responsible for developing and/or supporting IT applications and infrastructure.
6. A user's supervisor must notify the system administrator when a user's account is no longer needed or when access needs must change. The user's access is disabled within 24 hours.
    a. Logical access rights must be temporary disabled when:

i. Personnel do not need such access for a prolonged period in excess of 30 days because they are not working due to leave, disability or other authorized purpose.

ii. Personnel are suspended for greater than 1 day for disciplinary purposes.

7. The system administrator must monitor account usage to ensure that no account goes over 90 consecutive days without usage.

   a. The information system must be configured to automatically disable accounts if not used for 90 days.

8. The system owner or system administrator shall approve emergency access to sensitive IT systems for a predetermined period not greater than 30 days and notifies the ISO for oversight. If the emergency access request leads to changes in the user's access level, attributes for the account are included in the documentation and maintained on file.

   a. The information system must be configured to automatically terminate temporary and emergency accounts after a predetermined period not greater than 30 days.

9. The system owner (or designee) must keep all user account data, information and documentation associated with a user's logical access on file, in accordance with Department of Forestry's Records Management Policy and Procedure.

10. The system owner shall be responsible for ensuring:

    a. At least two individuals have administrative accounts to each IT system in order to help provide continuity of operations.

    b. System administrators have both an administrative account and at least one user account and that administrators use their administrative accounts only when performing tasking requiring administrative privileges.

    c. The disabling of accounts within 24 hours of notification when the accounts:

       i. Temporary accounts that are no longer required.

       ii. Have expired.

       iii. Are no longer associated with a user or individual.

       iv. Are in violation of organizational policy or

       v. Have been inactive for 90 days.

    d. The disabling of accounts of individuals who pose significant privacy or security risk to DOF must be disabled within 4 hours.

    e. Disabled accounts are retained in accordance with Department of Forestry's records retention policy.

    f. Activation of accounts or granting of privilege is based on:

       i. The principle of least privilege

       ii. Valid access authorization documentation

       iii. Intended system usage

       iv. Meeting the missions and business functions of DOF and

       v. In accordance with the Criminal History Checks located in Policy and Procedure 08-003 Human Resources Equal Opportunity And Employment Practices, background checks must be completed before (or as soon as feasible) to establishing user accounts.

    g. Users are not sharing accounts unless the system resides on a guest network.

    h. Access credentials, for internal IT systems, are delivered to the user in a confidential manner based on information already on file.

i. Access credentials, for Internet-facing only systems, must be securely delivered (e.g., by alternate channels such as U.S. Mail) to all external users of all sensitive external IT systems after confirming requests.

j. The information system automatically audits account creation, modification, and disabling, and termination actions and notifies, as required, appropriate individuals.

k. Access levels are associated with group membership, where practical, and that every system user account is a member of at least one user group.

l. Guest accounts are prohibited on sensitive IT systems.

m. All service and hardware accounts are documented, including, but not limited to granting, administering and terminating access.

i. If the service or hardware account is not used for interactive login with the system, the account is exempt from the requirement to change the password at the interval defined in Policy and Procedure 9-007 Identification and Authentication.

n. In cases where two-factor authentication cannot be used, the analysis of why two-factor authentication is not used must be documented.

11. The user of DOF systems shall ensure that:

a. Accounts are not being shared.

b. Initial passwords are changed upon first use.

c. Proper notification is given to system owners to temporarily disable access when the user will not need such access for a prolonged period in excess of 30 days due to leave, disability or other authorized purpose.

d. System use is within the policies and guidelines.

12. System administrators and the ISO or designee must investigate any unusual system access activities observed in logs or reported to them by staff and employees. Investigation activities shall include the following:

a. Monitor for atypical usage of information system accounts,

b. Report atypical usage to the ISO,

c. Track and monitor privileged role assignments (e.g., key management, network and system administration, database administration, and web administration).

13. A user's continued need for access to all IT systems must be reviewed at least on an annual basis.

a. System owners will advise users of the need to recertify a continued need for access to the system.

b. The user will advise supervisor by email of the need to recertify.

c. The supervisor will review the need and notify the system owner of the continued need.

14. The ISO shall require that its service provider(s) document and implement account management practices for requesting, granting, administering, and terminating accounts, including the following components:

a. For all internal and external IT systems:

i. Prohibit the use of shared accounts on all IT systems. Those systems residing on a guest network are exempt from this requirement.

ii. Disable unneeded accounts in a timely manner.

iii. Retain unneeded accounts in a disabled state in accordance with the agency's records retention policy.

iv. Associate access levels with group membership, where practical, and require that every system user account be a member of at least one user group.

v. Require that the system administrator and the ISO or designee investigate any unusual system access activities.

vi. Require the system and data owner approve changes to access level authorizations.

vii. Require that system administrators have both an administrative account and at least one user account and require that administrators use their administrative accounts only when performing tasks that require administrative privileges.

viii. Prohibit the granting of local administrator rights to users. The agency head may grant exceptions to this requirement for those employees whose documented job duties are primarily the development and/or support of IT applications and infrastructure. These exception approvals must be documented annually and include the agency head's explicit acceptance of defined residual risks.

ix. Require that at least two individuals have administrative accounts to each IT system.

x. The information system automatically audits account creation, disabling and termination actions and notifies, as required, appropriate individuals.

xi. Temporarily disable logical access rights when personnel do not need such access for a prolonged period in excess of 30 days because they are not working due to leave, disability or other authorized purpose.

xii. Disable logical access rights upon suspension of personnel for greater than one day for disciplinary purposes.

b. For all internal IT systems:

i. Require a documented request from the user to establish an account on any internal IT system.

ii. Complete any agency-required background check before establishing accounts, or as soon as practicable thereafter.

iii. Require confirmation of the account request and approval by the IT system user's supervisor and approval by the system owner or ISO to establish accounts for all sensitive IT systems.

iv. Require secure delivery of access credentials to the user based on information already on file.

v. Notify supervisors, Human Resources, and the system administrator in a timely manner about termination, transfer of employees and contractors with access rights to internal IT systems and data.

vi. Promptly remove access when no longer required.

c. For all external IT systems:

i. Require secure delivery of access credentials to users of all external IT systems.

ii. Require confirmation of the user's request for access credentials based on information already on file prior to delivery of the access credentials to users of all sensitive external IT systems.

iii. Require delivery of access credentials to users of all sensitive external IT systems by means of an alternate channel (i.e., U.S. Mail).

d. For all service and hardware accounts:

i. Document account management practices for all agency created service accounts, including, but not limited to granting, administering and terminating accounts. If the service or hardware account is not used for interactive login with the system, the service or hardware account is exempt from the requirement to change the password at the interval defined in the Password Management section of this standard.

e. If the IT system is classified as sensitive, prohibit the use of guest accounts.

f. If the IT system is classified as sensitive, require requests for and approvals of emergency or temporary access that:

i. Are documented according to standard practice and maintained on file

ii. Include access attributes for the account

iii. Are approved by the system owner and communicated to the ISO

iv. Expire after a predetermined period, based on sensitivity and risk

Access Enforcement (AC-3)

1. System administrators must enforce:
    a. Approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
    b. A role-based access control (RBAC) policy over defined subjects and objects and control access based upon organization-defined roles and users authorized to assume such roles.
2. System administrators may release information outside of the system only if:
    a. The receiving organization authorized system or system component provides security controls that meet Commonwealth security standards; and
    b. The organization-defined controls are used to validate the appropriateness of the information designated for release.
3. System administrators must restrict access to data repositories containing organization-defined information types.

Information Flow Enforcement (AC-4)

1. The system administrator must ensure that the information system enforces approved authorizations for controlling the flow of information within the system and between connected systems in accordance with applicable information flow policy.
    a. Flow control restrictions include, but are not limited to, the following:
        i. Blocking external traffic that claims to be from within the organization.
        ii. Keeping export-controlled information from being transmitted in the clear to the Internet.
        iii. Restricting web requests that are not from the internal web proxy server.
        iv. Limiting information transfers between organizations based on data structures and content.
    b. Flow control is based on the characteristics of the information and/or the information path.

        Note: Flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on content (e.g., using key word searches or document characteristics).

Separation of Duties (AC-5)

1. The system administrator separates duties of individuals as necessary, to prevent malevolent activity without collusion.
2. The system administrator is responsible for ensuring and documenting separation of duties.
3. The system administrator will implement separation of duties through assigned information system access authorizations.
4. Separation of duties include, but are not limited to, the following:
    a. Mission functions and distinct information system support functions are divided among different individuals/roles.
    b. Different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security).
    c. Security personnel who administer access control functions do not administer audit functions.
    d. Different administrator accounts for different roles.

Least Privilege (AC-6)

1. DOF shall employ the concept of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
    a. The System administrator is responsible for ensuring that each user has only enough access to conduct their job.
    b. The ISO explicitly approves and authorizes access to administrative or privileged accounts.
        i. Super-user accounts will be limited to system administration personnel.
    c. The system administrator requires that users of information system accounts, or roles, with access to administrative accounts, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.
    d. The system administrator prohibits privileged access to the information system by non-Department of Forestry users.
    e. The system administrator will review on an annual basis the privileges assigned to all users to validate the need for such privileges.
        i. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.
    f. The system administrator will log the execution of privileged functions.
    g. The system administrator will prevent non-privileged users from executing privileged functions.

Unsuccessful Login Attempts (AC-7)

1. ISO and the system administrator will implement a policy for unsuccessful logins. The policy shall be documented in the organization access control document and enforced automatically by the system.
    a. The information system will be configured to:
        i. Enforce a limit of a maximum of five consecutive invalid logon attempts by a user during a 15-minute period.
        ii. Automatically lock the account/node for a minimum period of 30 minutes when the maximum number of unsuccessful attempts is exceeded.
        iii. Automatically lock a sensitive account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.
        iv. Enforce a limit of five unsuccessful biometric login attempts.
        v. Allow DOF defined alternate authentication factors after primary methods have been attempted with a limit of five consecutive invalid logon attempts with an alternate method during a 15-minute period.
    b. These controls apply regardless of whether the login occurs via a local or network connection.
    c. The information system provides additional protection for mobile devices, such as smart phones or tablets, accessed via login by purging information from the device after ten consecutive, unsuccessful device logon attempts.
        i. This requirement may not apply to mobile devices if the information on the device is encrypted with sufficiently strong encryption mechanisms, making purging unnecessary.
        ii. The login is to the mobile device, not to any one account on the device. Therefore, a successful login to any account on the mobile device resets the unsuccessful login count to zero.

System Use Notification (AC-8)

1. The system administrator must notify users, both internal and external to the organization, with a notification message or banner that the monitoring of IT systems and data may include, but is not limited to, network traffic; application and data access; keystrokes (only when required for security investigations and approved in writing by the agency head); and user commands; email and Internet usage; and message and data content.
    a. The information system must be configured to:
        i. Display an approved system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable laws, directives, policies, regulations, standards and guidance and states that:
            - Users are accessing a Commonwealth of Virginia information system.
            - System use may be monitored, recorded and subject to an audit.
            - Unauthorized use of the system is prohibited and subject to criminal and civil penalties.
            - Use of the system indicates consent to monitoring and recording.
        ii. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.
        iii. Publicly accessible systems will:
            - Display the system use information, before granting further access to the publicly accessible system.
            - Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.
            - Include a description of the authorized uses of the system.

Concurrent Session Control (AC-10)

1. The system administrator is responsible for limiting the number of concurrent sessions for each server and database administrative account to five.

Device Lock (AC-11)

1. The system administrator is responsible for implementing a device locking policy that:
    a. Prevents further access to the system by initiating a device lock after 15 minutes of inactivity or upon receiving a request from a user.
    b. Retains the device lock until the user reestablishes access using established identification and authentication procedures.
    c. Conceals, via the device lock, information previously visible on the display with a publicly viewable image.

Session Termination (AC-12)

1. System administrator is responsible for implementing:
    a. An automatic termination for a user session after 24 hours of inactivity.
    b. A logout capability for user-initiated communication sessions whenever authentication is used to gain access to information resources.
    c. An explicit logout message to users, displayed to indicate the termination of authenticated communications sessions.

Permitted Actions without Identification or Authentication (AC-14)

1. It is the policy of the Commonwealth of Virginia to ensure that all system users be identified and authenticate to ensure proper access to the system. However, from time to time it may become necessary for a system to grant access without authentication. In these cases, the following must be adhered to:
    a. The system administrator is responsible for:
        i. Identifying and documenting specific user actions that can be performed without identification or authentication.
        ii. Documenting the supporting rationale in the System Security Plan.

Information Sharing (AC-21)

1. The ISO or designee shall require the following with regard to information sharing:
    a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for organization-defined information sharing circumstances where user discretion is required.
    b. Employ organization-defined automated mechanisms or manual processes to assist users in making information sharing and collaboration decisions.
    c. Employ organization-defined automated mechanisms to enforce information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.
    d. Implement information search and retrieval services that enforce organization-defined information sharing restrictions.

Publicly Accessible Content (AC-22)

1. The system owner is responsible to:
    a. Designate individuals authorized to post information onto an agency information system that is publicly accessible.
    b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.
    c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included.
    d. Review the content on the publicly accessible system for nonpublic information prior to initial posting, quarterly, and remove such information, if discovered.

Remote and Wireless Access

Remote Access (AC-17)

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. Department of Forestry shall ensure the following requirements are met:
    a. 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.
        i. All remote access will be monitored, and appropriate action is taken upon discovery of an unauthorized connection to the information system.

b. 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.

c. All users must protect information about remote access mechanisms from unauthorized use and disclosure.

d. All remote sessions for accessing sensitive data or development environments must employ two-factor authentication and be audited.

   i. 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.

e. All TCP and UDP ports except for explicitly identified components in support for specific operational requirements must be disabled.

f. When connected to internal networks from COV guest networks or non-COV networks, data transmission shall only use full tunneling and not split tunneling.

g. Protect the security of remote file transfer of sensitive data to and from agency IT systems by means of approved encryption.

h. Require that IT system users obtain formal authorization and a unique user ID and password prior to using the agency's remote access capabilities.

i. Document requirements for the physical and logical hardening of remote access devices.

j. Require maintenance of auditable records of all remote access.

k. Where supported by features of the system, session timeouts shall be implemented after a period of no longer than 15 minutes of inactivity and less, commensurate with sensitivity and risk. Where not supported by features of the system, mitigating controls must be implemented.

l. The organization ensures that remote sessions for accessing sensitive data or development environments employ two-factor authentication and are audited.

m. Any remote access of a DOF system from any device should be done via VPN if utilizing a public or guest Wi-Fi access.

Wireless Access Controls (AC-18)

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

1. The ISO or designee shall establish configuration requirements, connection requirements, and implementation guidance for wireless access implemented by the agency.

   a. Authorize each type of wireless access to the system prior to allowing such connections.

2. The following enhancements must be deployed for all wireless systems:

   a. 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.

   b. Wireless networking capabilities embedded within system components, when not intended for use, must be disabled prior to issuance and deployment.

   c. Users should not connect to guest wireless networks in any office location. Users should only connect to the designated, secure wireless connection.

   d. DOF guest wireless networks should only be used by authorized guests or visitors when using non-COV devices.

e. Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.

f. Monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points and will take appropriate action if an unauthorized connection is discovered.

g. Does not allow users to independently configure wireless networking capabilities, which include access points, authentication controllers, antennae, etc...

h. Does not allow users to create ad-hoc, peer-to-peer, or other unauthorized networks.

i. Allows users to use agency supplied mobile phones as a hot spot. Users should immediately connect to the VPN to access any sensitive systems.

3. The ISO or designee must ensure the following steps are followed and documented:

Wireless LAN (WLAN) Connectivity on the COV Network

a. The following requirements shall be met in the deployment, configuration and administration of WLAN infrastructure connected to any internal Commonwealth of Virginia network.

i. Client devices connecting to the WLAN must utilize two-factor authentication (i.e., digital certificates).

ii. WLAN infrastructure must authenticate each client device prior to permitting access to the WLAN.

iii. LAN user authorization infrastructure (i.e., Active Directory) must be used to authorize access to LAN resources.

iv. Only COV owned or leased equipment shall be granted access to an internal WLAN.

v. 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).

vi. Physical or logical separation between WLAN and wired LAN segments must exist.

vii. All COV WLAN access and traffic must be monitored for malicious activity and associated event log files stored on a centralized storage device.

viii. WLAN clients will only permit infrastructure mode communication.

WLAN Hotspot (Wireless Internet)

b. When building a wireless network, which will only provide unauthenticated access to the Internet, the following must be in place:

i. WLAN must have logical or physical separation from the agency's LAN.

ii. WLAN must have packet filtering capabilities enabled to protect clients from malicious activity.

iii. All WLAN access and traffic must be monitored for malicious activity, and log files stored on a centralized storage device.

iv. Where COV clients are concerned, WLAN clients will only permit infrastructure mode communication.

Wireless Bridging

c. The following network configuration shall be used when bridging two wired LANs:

i. 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 Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher).

ii. Wireless bridging devices will not have a default gateway configured.

iii. Wireless bridging devices must be physically or logically separated from other networks.

iv. Wireless bridge devices must only permit traffic destined to traverse the bridge and should not directly communicate with any other network.

v. Wireless bridging devices must not be configured for any other service than bridging (i.e., a wireless access point).

Mobile Device Access

Access Control for Mobile Devices (AC-19)

The director of IT shall establish usage restrictions and implementation guidance for DOF-controlled mobile devices.

1. The director of IT requires the following configuration, connection and usage requirements:
   a. The mobile device must be authorized by the director of IT.
   b. The mobile device must be registered with IT department.
   c. The mobile device user must read and sign the Agency Acceptable Use Policy (DHRM 1.75).
2. The ISO authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems.
   a. The mobile device must employ either full-device encryption or container encryption to protect the confidentiality and integrity of information on mobile devices.
   b. The mobile device user must not connect non-COV devices to the COV mobile device. Wall and vehicle charging devices and devices that provide sound input and output are permitted.
   c. The mobile device must not be attached to a non-COV computing system without the written permission of the agency head or designee.
   d. The mobile device must use only the boot ROM and operating system as supplied by the device vendor/carrier.
   e. The mobile device must only utilize software developed by the agency, a software vendor under contract to the agency or acquired via the device vendor's or suppliers' authorized application store.
   f. The mobile device must be configured to not allow the user to escalate the base privilege level.
   g. The mobile device user must not tamper with security controls configured on the device.
   h. The mobile device must install all security updates within 30-days of release by the original equipment manufacturer or the authorized device reseller.
   i. The mobile device shall only store sensitive COV data if approved by the agency head or designee.
   j. The mobile device must be configured to require all sensitive COV data be encrypted.
   k. The mobile device must be configured to allow a remote wipe of all COV data stored on the device.
   l. If the mobile device is lost or stolen, the incident must be reported to the DOF IT Help Desk and Commonwealth Security and Risk Management Incident Management within 24-hours in accordance with the Code of Virginia §2.2-603(F).
   m. The lost or stolen mobile device will be wiped within 24-hours of the incident. The wiping action will be initiated by a VCCC ticket.
   n. Any mobile device to be decommissioned or transferred to another employee must adhere to the COV ITRM Removal of Commonwealth Data from Electronic Media Standard SEC 514.
   o. The mobile device must be configured to store all COV data only on internal memory or non-removable media.

3. The ISO is responsible for enforcing requirements for the connection of mobile devices to organizational information systems.
    a. The mobile device must be configured to receive security policy and configuration information from the COV Mobile Policy Servers.
4. DOF will issue specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.
5. The system administrator applies organization-defined quarantine, inspection and preventative measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.
6. Users of mobile devices should use reasonable care in protecting mobile assets.
    a. The physical security of the mobile device is the responsibility of the employee to whom the device has been assigned.
    b. The mobile device must be protected at all times from unauthorized access.
    c. The mobile device must not be left unattended in any area accessible by the general public.
7. Users of non-COV owned mobile devices must follow these additional requirements:
    a. The device must only be used to access COV data via the COV Messaging Service, a web service accessible from the public Internet, or from a COV internal network in accordance with the COV ITRM IT Standard Use of Non-Commonwealth Computing Devices to Telework SEC 511. This requirement does not apply to the use of Outlook Web Access or restrict the use of the device for personal activities so long as those activities do not violate any other requirement of any existing COV policy.
    b. The mobile device user must agree in writing to allow remote wiping and the erasure of all COV data on the device without warning, if so, requested by the agency head or designee. The mobile device user must agree in writing to allow remote wiping and the erasure of all data on the device without warning if the COV data cannot be removed without wiping the entire device.
    c. The mobile device user must agree to surrender the device to Commonwealth Security for review and forensic imaging upon request of the associated agency head or the ISO.

Use of External Information Systems (AC-20)

Note: External information systems are information systems or components of information systems that are outside of the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness.

1. Department of Forestry employees and business partners who remotely access agency network resources will use only DOF provided equipment configured, set up and maintained by DOF without modification.
2. Access to network resources, including the Internet, will be via broadband or any other mode and Virtual Private Networking (VPN). This does not apply to users accessing Microsoft Outlook Web Access from a remote location.
3. The ISO shall limit the use of organization-controlled portable storage media by authorized individuals on external information systems.
4. Users are not allowed to use or store personal IT assets in facilities that house IT systems and data.

STATEMENT OF PROCEDURES

DOF procedures for New Access, Change in Access, Emergency Termination, Periodic Review of User Access, and Monitoring, Logging, and Investigation of Unusual Activity are outlined below.

New Access

Email, COV Network and IFRIS Access for New Users

Email and computer access is managed by VITA through the Commonwealth of Virginia (COV) Account Request process. IFRIS access is granted by HR and user roles (water quality, forester, etc.) are updated by the IT team based on the employee's job role provided by HR.

New employees and re-hires are granted email and computer access after their initial on-boarding with HR.

- HR informs the IT team of the new hire and IT team requests a new COV account using VCCC request.
- The IT team emails the supervisor to confirm appropriate file share access, distribution list and IFRIS access.
- The DOF ticket is assigned to an IFRIS system administrator who grants IFRIS role access, documents the changes in the DOF ticket and then closes the DOF ticket.

Other DOF Systems

New users may need access to other DOF systems depending on their position and role at DOF.

- The supervisor emails the designated system owner to request access.
- The system owner reviews the request and if approved forwards the access request to the system administrator.
- The system administrator changes access to the system and informs the system owner and the supervisor.

Modifications To Existing Access

Changes can occur due to a modification in role or position within the agency or a temporary change in functional assignment. If the change is for an employee role or employment status, it should initiate with HR. If it is another user type (contract, volunteer, wage, etc.), the supervisor will route through HR. For modification to existing network access, requests will include the business owner for the area that is being requested access.

Email, COV Network and IFRIS Access

- The supervisor emails HR and the IT team with requested changes.
- The IT team completes the online VCCC Form for changes to network access and email distribution lists.

Other DOF Systems

Changes to roles or positions may require changes in access within other DOF information systems. The steps of this procedure are the same as for new access.

- The supervisor emails the system owner for access change approval.
- The system owner reviews the request and if approved forwards the access request to the system administrator and IT Team.
- The system administrator changes access to the system and emails the IT team, the system owner and the supervisor.

Termination

Email, COV Network and All Other System Access

When employees leave the agency, access to COV network and all other systems will be terminated within one business day of the last day of work.

- The supervisor emails HR and the IT Team with termination information including the last day of employment.
- The IT teams confirms with the supervisor on data and email retention needs and completes a VCCC request accordingly.

Emergency Termination

Emergency termination occurs when a user's access rights need to be terminated immediately due to possible compromise of security. Emergency termination or account lock requests must be routed through HR.

- The supervisor sends a request by email to HR with subject line "Emergency Account Termination."
- HR sends/forwards the emergency termination request to IT Team and ISO.
- The IT team creates a VCCC to request urgent account disable and receives the VCCC ticket number.
- The IT team emails the termination requests to affected system owners and/or system administrator.

Periodic Review of User IDs

- By October 31 of each year, all supervisors will review active and inactive DOF user IDs by completing the annual access renewal form. The annual access renewal form is submitted to the ISO. The ISO will verify employee's receipt of acceptable use agreement (DHRM Policy 1.75).
  - The following criteria are used to support the need to continue a user's access or access level:
    - Confirmation of continuing employment
    - Confirmation of current roles and responsibilities and/or any changes
    - Confirmation of current access levels and/or needed changes
    - Confirmation of annual receipt of DHRM Policy 1.75 Use of Electronic Communications and Social Media.
  - Any needed changes are made and the appropriate individuals, such as system owners/system administrator are notified as necessary.
- User access is reviewed for inactivity every 90 days by system administrator. If a user has not accessed an account in 90 days, access is suspended/terminated, and user is emailed of the change.
  - Exceptions to the standard period above include extended medical leave.
- The process for reactivating a disabled user's access is as follows:
  - Supervisor must contact IT Team to inform them of the change and need for reactivation.

Monitoring, Logging, and Investigation of Unusual Activity

DOF monitors and logs access to application and related database files according to the process outlined below:

- The monitoring and logging of access to application and related data base files is accomplished through the SPLUNK platform.
- System administrator and ISO will monitor/have access to the logs.
  - Logs will be monitored monthly.
  - System owners will be notified by email of unusual activity or unauthorized access.
  - Investigation and reporting of unusual activity and/or unauthorized access will be done in accordance with the Policy and Procedure 09-008 Information Security Incident Response.

AUTHORITY

This policy and procedure is issued by the Virginia state forester.

INTERPRETATION

The director of information technology and chief of administration are responsible for the interpretation of this policy and procedure.

APPROVAL

I certify that this policy and procedure is approved and ready for publication.

Parik Patel	DocuSigned by: Parik Patel 3448F7C5358F457... 7/2/2024
Director of Information Technology Name (Print)	Director of Information Technology Signature
Amanda Davis	DocuSigned by: amanda davis C2CCAB60F85A4A0... 7/9/2024
Chief of Administration Name (Print)	Chief of Administration Signature

VERSION HISTORY

Version History			
Date	**Version**	**Details**	**Author/Contributors**
May 22, 2024	1	Original – Based on CSRM Template (version 12.29.2021) and updated with SEC530 standards	Catherine Shefski, ISO