Division of Enterprise Technology Strategy and Services

ETSS Policy 300.1

Access Control (AC)

Publish Date: 23 June 2026
Effective Date: 23 June 2026
Last Review: 22 June 2026

doa.entsec@doit.ri.gov

1. Purpose

Establish policy for implementing and managing logical and physical access controls that safeguard State of Rhode Island information systems, infrastructure, and data. This policy ensures that only authorized users, devices, and processes gain access commensurate with business need; that privileged actions are tightly governed and auditable; and that accountability for user actions is maintained.

This policy directly supports the Govern and Protect functions of NIST CSF 2.0 and implements the AC control family of NIST SP 800-53 Rev.5 (Moderate) within the State's ETSS Security & Risk Program (PM-1) and NIST RMF. It recognizes Complementary User Entity Controls (CUECs) by defining shared responsibilities for Agencies, vendors, and cloud service providers (CSPs) operating on behalf of the State.

2. Applicability

This policy is applicable to all State of Rhode Island Executive Branch Departments[1] (including agencies, boards and commissions), and their employees (including permanent, non-permanent, full-time, and part-time) and interns, consultants, contractors, vendors, contracted individuals, and any entity having access to state information systems and data, whether operated or maintained by the state or on behalf of the state. For this policy, the term "agency" is used to refer to any department, agency, division, or unit of the Executive branch of the State of Rhode Island.

3. Roles and Responsibilities

3.1. **State CISO (ETSS):** Owns this policy; approves exceptions; oversees enterprise access strategy, monitoring, and enforcement.

3.2. **System Owner / Data Owner:** Defines access needs/roles, approves access (including privileged), ensures periodic reviews.

3.3. **Agency Information Manager (AIM)/Technical Support Manager (TSM) (ETSS Agency IT support)**: Authorizes users, remote access, and wireless deployments; ensures local compliance.

Related Policies: ***Enterprise Policies***

3.4. **ETSS Enterprise Teams (Identity and Access Management (IAM), Network, Security Operations):** Operate centralized Identity platform (e.g., Entra ID), enable Conditional Access, MFA, VPN, Privileged Access Management (PAM), logging/monitoring, and alert response.

3.5. **Vendors/CSPs:** Implement CUECs and contractually required controls; provide attestation/evidence.

3.6. **All Non-privileged Users:** Use unique credentials, protect authentication factors, and comply with acceptable use and access policies.

4. Procedures for Compliance

Security controls in this policy will be implemented in accordance with the security categorization of the information system. The security categorization is based on the Information Assurance Level (IAL) requirements of the information system.

Low Risk Systems (IAL1)
Information systems that only contain data that is public by law or directly available to the public via mechanisms such as the internet. In addition, desktops, laptops, and supporting systems used by agencies are Low Risk unless they store, process, transfer, or communicate private or sensitive data.

Moderate Risk Systems (IAL2)
Information systems that store, process, transfer, or communicate private or sensitive data or have a direct dependency on a Moderate Risk system. At a minimum, any information system that stores, processes, transfers, or communicates PII or other sensitive data types is classified as a Moderate Risk system.

4.1. ***[IAL1, IAL2]*** **Access Control Policy and Procedures (AC-1).** ETSS establishes, disseminates, and annually reviews access control policy and procedures. Agencies must document system-specific procedures within their System Security Plans (SSPs) and align with enterprise identity, PAM, MFA, and logging standards.

4.2. ***[IAL1, IAL2]*** **Account Management (AC-2).** ETSS and the agency shall:

1. Identify and document allowed accounts and accounts specifically prohibited for use within the information system to support agency mission and business functions, including individual, group, system, application, guest, emergency, and temporary accounts. Privileged accounts will only be assigned to personnel that require elevated levels of access to perform their job functions.

2. Assign account managers for information system accounts.

3. Establish conditions and criteria for group and role membership (Role Based Access Control (RBAC). Service accounts will be used for processes, such as application execution, automated services, and virtual machine instances, that perform actions on behalf of human users and that are not tied with the lifecycle of human/individual user accounts. Individual user accounts will not be used to perform system actions that should be performed by service accounts.

4. Identify authorized users of the information system. Each information system user will have a unique user identification for accessing the system. User identifications that do not provide unique individual user-level audit information (e.g. generic accounts, guest accounts, shared accounts) should be limited and well controlled. An up-to-date record of all users, including guest/generic/shared accounts, authorized to access the information system will be maintained by the agency.

5. Specify access privileges for each information system account. Access privileges assigned to external users (e.g. vendors, contractors) will be commensurate with access restrictions of the respective agency information system.

6. Require approval from authorized personnel for requests to create information system accounts. Privileged user accounts require approval from the system owner prior to access being granted.

7. Create, enable, modify, disable, and remove information system accounts in accordance with ETSS and agency account management procedures. Where possible, this process should be automated by the information system. Inactive or unused default information system accounts will be disabled or removed. Default passwords of default information system accounts will be changed in accordance with ETSS Identification and Authentication Policy.

8. Monitor the use of information system accounts. Users will not share their account information with other users. User accounts will be monitored for indications of compromised or shared accounts.

9. Notify system owner or ETSS agency support team within five (5) business days when user accounts are no longer required, upon a transfer or termination of employment, or upon changes to information system usage or need-to-know requirements. The support member will promptly submit a service ticket request that the system administrator delete the account from the information system.

10. Authorize access to information systems based on a valid access authorization, intended system usage, and permissions required by the agency or associated mission and business functions.

11. Annually review information system accounts for compliance with account management requirements. Privileged accounts will be reviewed semi-annually.

12. Establish a process for reissuing shared/group account credentials when individuals are removed from the group.

4.2.1. [IAL2] **Automated System Account Management (AC-2.1).** ETSS and the agency will employ automated mechanisms to support the management of information system accounts.

4.2.2. [IAL2] Automated Temporary and Emergency Account Management (AC-2.2). The information system will automatically:

1. Disable temporary and emergency accounts within two (2) business days following the resolution of the issue that required their use.

2. Remove temporary accounts within no more than six (6) months from the date the temporary account was created. Temporary accounts will not be created without a corresponding expiration date.

4.2.3. [IAL2] Disable Accounts (AC-2.3). ETSS and the agency will disable:

1. Non-privileged accounts (e.g. user, device, service accounts) after ninety (90) days of inactivity.

2. Privileged accounts (e.g. user, device, service accounts) after sixty (60) days of inactivity.

3. Expired accounts.

4. Accounts no longer associated with a user, contractor, or vendor.

4.2.4. [IAL2] Automated Audit Actions (AC-2.4). The information system will automatically audit account creation, modification, enabling, disabling, and removal actions, and promptly notify system administrators of these actions.

4.2.5. [IAL2] Inactivity Logout (AC-2.5). The agency will require that users log out when they are expecting periods of inactivity greater than one (1) hour unless the logout would cause a critical process to terminate prematurely.

4.2.6. [IAL2] Disable Accounts for High-Risk Individuals (AC-2.13). The agency will disable the account of high-risk and privileged users within one (1) hour of the discovery of a significant risk associated with the account including, but not limited to, suspected compromised credentials, or unauthorized access to PII and other confidential or sensitive data.

4.3. [IAL1, IAL2] Access Enforcement (AC-3). The information system will:

1. Limit and enforce approved authorizations of users, processes acting on behalf of authorized users, and devices (including other systems) logically accessing the information system or system resources. State network access will be administered and enforced via a centralized access control system (e.g. Microsoft Active Directory or EntraID) that leverages user, group, and role-based access to information resources. For information systems and applications that do not leverage the centralized access control system, system owners are responsible for enforcing approved authorizations of users, processes acting on behalf of users, and devices (including other systems). Contracted external service providers will isolate PII, including applications and services that receive, process, store, or transmit PII, within the service provider environment to the extent that other service provider customers that share physical or virtual space cannot gain access to PII, applications, or services.

2. Limit the execution of functions and transactions to only those that authorized users are permitted to execute.

3. Identify and authenticate each user, process acting on behalf of an authorized user, and device (including other systems) prior to granting system access. The authentication method used will be commensurate with the sensitivity of the information system and data being accessed. If encryption is used as an access control mechanism, it must meet FIPS 140-2 or FIPS 140-3 (as applicable during the *transition* period) encryption standards documented in ETSS System and Communications Protection Policy.

4. Maintain the identity of all active users.

5. Link system actions to individual users.

4.4. ***[IAL2]*** **Information Flow Enforcement (AC-4).** The information system will enforce approved authorizations for controlling the flow of information within the system and between interconnected systems based on the technical safeguards in place to protect the information. System and data owners, in coordination with enterprise information technology personnel, will define information flow control policies, methods, and enforcement mechanisms that enforce defined approved authorizations. Information flow may include tactics such as designating sources and destinations (e.g. networks, individuals, devices), prohibiting information transfers between connected systems (e.g. allowing access only), verifying write permissions prior to accepting information from another information system, employing hardware mechanisms to enforce one-way information flows, implementing mechanisms that reassign security or privacy attributes and labels that are enforced via, blocking external traffic that claims to be from within the state network, keeping controlled information and PII from being transmitted in the clear within the public domain (i.e. internet), restricting web requests that are not from internal web proxy servers, and limiting information transfers between the state and external entities based on data structures and content. The enforcement of information flow may be implemented via, for example, routing, DNS, and boundary protection devices (e.g. employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content).

4.5. ***[IAL2]*** **Separation of Duties (AC-5).** Agency policies, procedures, and standards that address agency-specific business needs and regulatory/compliance requirements will support separation of duties to ensure the confidentiality, integrity, and availability of agency information systems and data. The agency will define information system access authorizations that support separation of duties and reduce the risk of malevolent activity or collusion, as well as identify, document, and separate the duties of individuals requiring separation, including:

1. Ensuring audit functions are not performed by the same personnel responsible for administering access control.

2. Ensuring financial transactions are not entered by the same individual who is responsible for authorizing a payment based on the transaction.

3. Limiting the number of system administrators and basing access in accordance with the user's role and responsibilities.

4. Ensuring mission critical functions and information system support functions are appropriately segregated. Unless approved by an authorized individual, source code developers will not release their own code for mission critical information systems or systems where there is a high risk of fraud being committed.

5. Ensuring testing and production functions (e.g. user acceptance, quality assurance, information security) are performed by appropriate individuals/groups. Source code will be committed to an approved repository for review and approval by an authorized individual prior to the code being released into a production environment.

6. Ensuring information system security testing is performed by an independent authority (e.g. not the business process owner, system owner, system developers, system administrators).

4.6. ***[IAL2]*** **Least Privilege (AC-6).** The agency will employ the principle of least privilege and allow only authorized access for users (or processes acting on behalf of users) necessary to accomplish assigned tasks in accordance with agency mission and business functions, including:

1. Restrict privileged information system accounts to individuals who require privileged access to perform their administrative duties.

2. Require privileged users to use non-privileged accounts when accessing non-security functions.

3. Restrict database management utilities to authorized database administrators.

4. Permit only authorized users to access files, directories, drives, workstations, servers, network shares, ports, protocols, and services required to perform their job duties.

5. Provide vendors and contractors with minimal information system and physical access, in accordance with documented ETTS policies and security requirements.

6. Disable information system file system access not explicitly required for system, application, or administrator functionality.

7. Disable information system and removable media boot access unless explicitly authorized by the State CISO for operational requirements (if authorized, boot access will be password protected).

4.6.1. ***[IAL2]*** **Authorize Access to Security Functions (AC-6.1).** The agency will identify security functions and explicitly authorize access for privileged account users to security functions deployed in hardware, software, firmware, and other security-relevant information, including the configuration or modification of audit logs, auditing behavior, boundary protection rules, access authorizations (e.g. permissions, privileges), authentication parameters (e.g. password complexity), system configurations and parameters.

4.6.2. ***[IAL2]*** **Non-Privileged Access for Non-Security Functions (AC-6.2).** The agency will identify non-security functions and require that users of information system accounts (or roles) with access to security functions and security-relevant information use non-privileged accounts (or roles) when accessing non-security functions.

4.6.3. ***[IAL2]*** **Privileged Accounts (AC-6.5).** The agency will identify privileged accounts on the information system and restrict these accounts to designated personnel (or roles) only. Privileged accounts include, but are not limited to, security administrators, system and network administrators, system maintenance personnel, system programmers, and other roles that require elevated privileges.

4.6.4. ***[IAL2]*** **Review of User Privileges (AC-6.7).** The agency will review account privileges annually to validate the need for such privileges. Unnecessary permissions will be promptly removed to reflect agency business requirements.

4.6.5. ***[IAL2]*** **Log Use of Privileges Functions (AC-6.9).** The agency will audit the execution of privileged functions.

4.6.6. ***[IAL2]*** **Prohibit Non-Privileged Users from Executing Privileged Functions (AC-6.10).** The information system will prevent non-privileged users from executing privileged functions, including the disabling, circumventing, or altering of implemented security safeguards/countermeasures. The agency will define privileged functions and non-privileged users.

4.7. ***[IAL1, IAL2]*** **Unsuccessful Logon Attempts (AC-7).** The information system will automatically lock user accounts after three (3) consecutive invalid logon attempts. Privileged accounts will remain locked until unlocked by a system administrator. Non-privileged accounts may be automatically unlocked after a minimum of fifteen (15) minutes. However, upon six (6) consecutive invalid logon attempts, non-privileged accounts will remain locked until unlocked by a system administrator.

4.8. ***[IAL1, IAL2]*** **System Use Notification (AC-8).** The information system will:

1. Display a system use notification message (i.e. warning banner) on the screen at each login attempt prior to granting system access that provides users with general policy on system use, prohibited activities, and privacy or security concerns consistent with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system owner determines the elements of the environment that require the system use notification control.

2. Display the system use notification on screen until the user acknowledges and explicitly agrees to the displayed message.

<u>Non-Public Information Systems</u>
Prior to granting system access, the information system will display a system use notification message that states:
(a) The user is accessing a State of Rhode Island government information system.
(b) System use is monitored, recorded, and subject to audit.

(c) Use of the system implies user consent to being monitored and recorded.
(d) Unauthorized use of the system is prohibited and subject to criminal and civil penalties.

Publicly Accessible Information Systems
Prior to granting system access, the information system will display a system use notification message that:
(a) Displays system use conditions.
(b) References monitoring, recording, or auditing activities are consistent with privacy accommodations for the system.
(c) Includes a description of the authorized use of the system.

4.9. ***[IAL2]*** **Device Lock (AC-11).** The information system will automatically prevent further access to the system by initiating a session lock after no more than fifteen (15) minutes of inactivity. The session lock will remain in place until the user re-authenticates to the system in accordance with established identification and authentication procedures (e.g. login with username and password).

4.9.1. ***[IAL2]*** **Pattern-Hiding Displays (AC-11.1).** The information system will conceal, via the session lock, data previously displayed on the screen with a publicly viewable image. The pattern-hiding display will not display non-public data but can include static or dynamic images, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen.

4.10. ***[IAL2]*** **Session Termination (AC-12).** The information system will automatically terminate user-initiated sessions after no more than thirty (30) minutes of inactivity, upon a user logoff, or other agency-defined conditions or events (e.g. concurrent session limits, timed intervals, session connection duration, location, etc.).

4.11. ***[IAL1, IAL2]*** **Permitted Actions without Identification or Authentication (AC-14).** For non-public information systems, no actions will be performed without the user being identified and authenticated. For publicly accessible information systems, only public content (i.e. public data) may be accessed without the user being identified. User actions not requiring identification and authentication will be documented in the SSP.

4.12. ***[IAL1, IAL2]*** **Remote Access (AC-17).** Mechanisms that provide remote access to the internal state network, including the Enterprise VPN solution, will be managed and maintained by ETSS Enterprise Team personnel. MFA is required for all remote access to the state network. The agency will:

1. Authorize remote access to agency information systems via an external network (e.g. internet) prior to granting such connections. Only ETSS-approved VPN clients are authorized. The agency will not implement any non-ETSS approved remote access solution that grants access to the state network or information system without prior written approval from the ETSS CISO and CTO.

2. Monitor unauthorized remote access to the information system. Remotely accessing the state network from a location outside of the United States or one of its territories is **not** authorized without prior approved International Travel Request.

3. Establish and document usage restrictions, configuration and connection requirements, and implementation guidance for each type of remote access method allowed. At a minimum, all computers and devices, whether state or contractor-owned, that require remote access to the state network will be securely configured and have up-to-date system patches installed, up-to-date anti-virus software installed, ensure that functionality the allows the automatic execution of unauthorized code is disabled. Devices will be scanned for compliance with these requirements prior to a remote connection to the state network being established.

4. For the Enterprise VPN solution:

a. **Authority.** ETSS Enterprise is solely responsible for maintenance and administration of the VPN solution for remote access to the state network. Agencies will not implement any VPN access without prior approval from the ETSS CISO.

b. **Approvals.** VPN access will be authorized and approved by the Agency Information Manager (AIM) or Technical Support Manager (TSM) and appropriate ETSS operational management prior to access being granted. VPN access will only be approved for valid business uses.

c. **Users.** VPN accounts will only be created for users that have been authorized and approved for remote access to the state network. Users will not share their account user ID and password with anyone and are responsible for ensuring that unauthorized users do not access the state network via their VPN account. VPN users will notify agency IT technical support personnel or ETSS Service Desk immediately upon becoming aware of a compromised account.

d. **Authentication.** VPN account passwords will adhere to password complexity requirements documented in ETSS Identification and Authentication Policy. MFA will be used for all remote access to the state network via the Enterprise VPN solution. For IRS-audited agencies that process, store, or transmit FTI, any user that does not own a personal smartphone and has not been assigned a state-owned smartphone by the agency OR the user owns a personal smartphone but declines to install the required third-party MFA application on his/her personal smartphone. users requiring remote access via the state's VPN solution will be issued a physical token for remote access.

e. **Devices.** Unless approved by the ETSS, only state-owned devices will be allowed to remotely access the state network via the state's VPN solution. Personal and vendor-owned devices intended to be used for remote access to the state network must be approved for use in alignment with the ETSS Bring Your Own Device (BYOD) Program and will comply with all ETSS policies and procedures.

f. **Sessions.** Only state-approved VPN clients are authorized. Unless approved by the agency for a state-provided wireless access point, VPN users will be responsible for providing an internet connection for VPN access. Users with active VPN sessions have no expectation of privacy and will be monitored for compliance with ETSS policies and standards. VPN sessions will be limited to one (1) active connection per user and will automatically terminate after ten (10) minutes of inactivity. VPN users will be required to re-authenticate after a session is terminated for any reason. VPN connections will have a maximum absolute connection time of eight (8) hours unless authorized and approved by the VPN system administrator to extend the absolute connection time limit beyond eight (8) hours (extensions require valid business use justification). While actively connected to the state network via VPN, all traffic to and from the remotely attached device will be forced through the encrypted VPN tunnel. Split-tunneling is not allowed unless authorized and approved by the State CISO.

4.12.1. ***[IAL2]*** **Monitoring and Control (AC-17.1).** The agency will employ automated mechanisms to monitor and control remote access sessions to ensure policy compliance of remote connection activities to information system components (e.g. servers, workstation, tablets, smartphones).

4.12.2. ***[IAL2]*** **Protection of Confidentiality and Integrity using Encryption (AC-17.2).** The agency will implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. Any application that remotely accesses the information system will use an approved encryption method. The encryption strength used will be commensurate with the confidentiality and integrity requirements of the data. See ETSS System and Communications Protection Policy for more information.

4.12.3. ***[IAL2]*** **Managed Access Control Points (AC-17.3).** The agency will route all remote access to the information system through a limited number of ETSS-managed network access control points (e.g. firewalls, routers, switches). Access control points will be managed and maintained by ETSS.

4.12.4. ***[IAL2]*** **Privileged Commands and Access (AC-17.4).** The agency will authorize, and document, within the SSP, the execution of privileged commands and access to security-relevant information via remote access. Only privileged commands and security-relevant information identified in the SSP may be executed or accessed via remote access.

4.13. ***[IAL1, IAL2]*** **Wireless Access (AC-18).** ETSS Enterprise will install, configure, and centrally manage all wireless access and APs authorized to connect to the state network. All wireless AP installations, removals, or location changes require a request for change and must be formally approved by the ETSS Change Approval Board (CAB). The AIM will authorize and approve all wireless APs installed within agency facilities. The system owner will authorize wireless access to the information system prior to allowing wireless connections. Agency IT personnel will notify ETSS Network and Security teams immediately upon discovery of an unauthorized AP installed within agency facilities. ETSS will establish usage restrictions, configuration and connection requirements, and implementation guidance for wireless access, including:

1. Wireless APs will be installed within secure areas that are not publicly accessible. If this is not possible, the AP will be secured by a tamper-resistant enclosure.

2. Static IP addresses will be assigned to wireless APs. Dynamic Host Configuration Protocol (DHCP) will not be used for this purpose.

3. SSID's for internal use by ETSS Colleagues (non-guest use) will not be broadcast openly. ETSS will document all approved SSID's and associated configuration criteria.

4. Wireless devices will be authenticated via their MAC address.

5. Wireless device users will:

a. Disable wireless networking capabilities of wireless-capable devices when wireless access is not required.

b. Physically secure wirelessly connected devices within state-owned facilities and when in public areas.

c. Verify they are connecting to an authorized state wireless network SSID prior to connecting to the wireless network. If you are unsure, please contact the ETSS Service Desk for verification.

4.13.1. [IAL2] **Authentication and Encryption (AC-18.1).** The information system will be configured to protect wireless access to the system via the use of encryption mechanisms and authentication of users or devices. Wireless communications will be encrypted using a FIPS 140-2 or FIPS 140-3 (as applicable during the *transition* period) validated encryption module in accordance with ETSS System and Communications Protection Policy. Users connecting to a state wireless access SSID that grants access to the internal network will be authenticated prior to being granted access.

4.13.2. [IAL2] **Disable Wireless Networking (AC-18.3).** The agency will disable wireless networking capabilities embedded within system components prior to issuance and deployment if the wireless networking capability is not to be used. ETSS, at its sole discretion, has the authority to disable any wireless AP or sever any wireless connection that it has determined to pose a security threat. ETSS will perform periodic sweeps of the state wireless network to identify rogue access points, including periodic vulnerability scanning of wireless Access Points (AP's).

4.14. [IAL1, IAL2] **Access Control for Mobile Devices (AC-19).** ETSS and the agency will:

1. Establish usage restrictions, configuration requirements, and connection requirements for agency controlled mobile devices.

2. Authorize the connection of mobile devices to agency information systems.

4.14.1. [IAL2] **Full Device or Container-Based Encryption (AC-19.5).** The agency will employ FIPS 140-2 or FIPS 140-3 (as applicable during the *transition* period) validated encryption to protect the confidentiality and integrity of confidential or sensitive data, including PII, maintained on mobile devices. All state-owned mobile devices will be encrypted unless an exception is formally approved in writing by the ETSS CISO.

4.15. [IAL1, IAL2] **Use of External Systems (AC-20).** External information systems are systems that are outside the authority of the agency and direct control of the implementation of security controls over the systems (e.g. infrastructure/software/platform as a service cloud services, personally owned computers and smartphones). The agency will identify, verify, and control the use of and connections to external information systems, including establishing terms and conditions under which authorized users can:

1. Access non-public interfaces of agency information systems from external information systems. All personnel (e.g. employees, vendors, contractors) working from an external location will implement fundamental security controls and practices, including using complex passwords, installing malware and virus protection, and enabling personal firewalls. Remote access will be limited to information resources that are necessary to complete required job duties.

2. Process, store, or transmit agency data using external information systems. External information systems must meet security control standards required by ETSS and the agency, as well as follow applicable legally binding data sharing agreements. Agency data owners will perform a risk assessment for data under their control prior to allowing the use of an external information system to process, store, or transmit the data. The AIM will maintain a list of currently approved external information systems.

4.15.1. *[IAL2]* **Limits on Authorized Use (AC-20.1).** The agency will authorize individuals to use external information systems to access the information system or process, store, or transmit agency data only when the agency:

1. Verifies that required security controls are implemented on external information systems. Depending on the confidence level required, verification can be achieved via third-party reviews, independent assessments, or other attestation.

2. Maintains approved information system connection or processing agreements with the organization hosting the external information system.

4.15.2. *[IAL2]* **Portable Storage Devices – Restricted Use (AC-20.2).** The agency will restrict the use of agency-controlled portable devices on external information systems. Only state-owned portable storage devices can be used to process, access, and store PII and other confidential or sensitive data. These storage devices will employ encryption to protect the confidentiality and integrity of the data.

4.16. *[IAL2]* **Information Sharing (AC-21).** ETSS and the agency will:

1. Restrict the sharing of information (e.g. medical, contract, proprietary, PI, or other confidential, sensitive, or controlled information) in accordance with in 45 CFR §155.260 (e) by identifying appropriate information access restrictions and authorizations, identifying the individuals or groups within the agency authorized to share the information, and the circumstances under which the information may be shared and where discretion is required. Agency data owners will annually review access levels of all authorized users, including external users that have access to agency data being processed, stored, or transmitted on external information systems.

2. Employ automated mechanisms or manual processes within the applicable SSP to assist users in making information-sharing/collaboration decisions.

4.17. ***[IAL1, IAL2]*** **Publicly Accessible Content (AC-22).** The agency will:

1. Identify publicly accessible information resources.

2. Designate business information owner(s) who are responsible for publicly accessible information resources under their control.

3. Designate and train individuals authorized to post information on publicly accessible information systems and websites.

4. Review the information prior to posting onto publicly accessible information systems and websites to ensure only public information is included. The business information owner may designate one or more information custodians who are responsible for ensuring that only public data is posted to publicly accessible information systems and websites.

5. Review content posted on publicly accessible information systems and websites every three (3) months for non-public data and, if discovered, remove such information no more than (1) week following the time of discovery. The business information owner is responsible for documenting content review procedures on publicly accessible information systems and websites for data under their control.

5. Approval / Review Signature:

Sanjay Gupta
Digitally signed by Sanjay Gupta
Date: 2026.06.22 16:34:53 -04'00'

Chief Technology Officer (CTO)
Division of Enterprise Technology Strategy and Services (ETSS)

Digitally signed by Nathan Loura
Date: 2026.06.23 12:24:02 -04'00'

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

Brian Tardiff
Digitally signed by Brian Tardiff
Date: 2026.06.23 12:42:48 -04'00'

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