5.5 Access Control (AC) Policy

PURPOSE

To ensure that access controls are implemented and in compliance with IT security policies, standards, and procedures. Access controls provide the planning and implementation of mechanisms to restrict reading, writing, processing, and transmission of CJIS information and the modification of information systems, applications, services, and communication configurations allowing access to CJIS information.

POLICY

This policy is applicable to all departments and users of *[agency name]* resources and assets.

01. ACCOUNT MANAGEMENT

1. Identify and select the following types of information system accounts to support organizational missions and business functions: individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.
2. Assign account managers for information system accounts.
3. Establish conditions for group and role membership.
4. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.
5. Require approvals by system owners for requests to create information system accounts.
6. Create, enable, modify, disable, and remove information system accounts in accordance with approved procedures.
7. Monitor the use of information system accounts.
8. Notify account managers within one day when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes.
9. Authorize access to the information system based on a valid access authorization, intended system usage, and attributes from (d).
10. Review accounts for compliance with account management requirements at least annually.
11. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
12. Align account management processes with personnel termination and transfer processes.
13. Employ automated mechanisms to support the management of information system accounts within 72 hours.
14. Ensure that the information system automatically disables temporary and emergency accounts after usage.
15. Ensure that the information system automatically disables inactive accounts within one week when the accounts have expired, are no longer associated with the user/individual, are in violation of organizational policy, or have been inactive for 90 calendar days.
16. Ensure that the information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate IT personnel.
17. Require that users log out when a work period has been completed.
18. Disable accounts of individuals within 30 minutes of discovery of direct threats to the confidentiality, integrity, or availability of CJI.

02. ACCESS ENFORCEMENT

1. The [*agency name*] in collaboration with the [*IT department*] shall:
2. Ensure that the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

03. INFORMATION FLOW ENFORCEMENT

1. Ensure that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on applicable policy.

04. SEPARATION OF DUTIES

1. Identify and document separation of duties based on specific duties, operations, or information systems, to mitigate risk to CJI.
2. Define system access authorization to support separation of duties.

05. LEAST PRIVILEGE

1. Employ the principle 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.
2. Authorize access for personnel including security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information security personnel, maintainers, system programmers, etc.) to establish system accounts, configured access authorizations, set events to be audited, set intrusion detection parameters, and other security functions, and security-relevant information in hardware, software, and firmware.
3. Require that users of system accounts, or roles, with access to privileged security functions or security relevant information (i.e., audit logs), use non-privileged accounts or roles when accessing non-security functions.
4. Restrict privileged accounts on the information system to privileged users.
5. Annually review the privileges assigned to privileged and non-privileged users to validate the need for such privileges and reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.
6. Log the execution of privileged functions.
7. Prevent non-privileged users from executing privileged functions.

06. UNSUCCESSFUL LOGON ATTEMPTS

1. Enforces a limit of five consecutive invalid logon attempts by a user during a 15-minute time period.
2. Automatically locks the account until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

07. SYSTEM USE NOTIFICATION

1. Displays to users an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable state and federal laws, directives, policies, regulations, standards, and guidance and states informing that:
2. Users are accessing a restricted information system.
3. System usage may be monitored, recorded, and subject to audit.
4. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties.
5. Use of the information system indicates consent to monitoring and recording.
6. 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 information system.
7. For publicly accessible systems, the [*agency name*] shall ensure that the information system:
8. Displays system use information consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines, before granting further access to the publicly accessible system.
9. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.
10. Includes a description of the authorized uses of the system.

08. SESSION/DEVICE LOCK

1. Prevent further access to the system by initiating a device lock after a maximum of 30 minutes of inactivity and requiring the user to initiate a device lock before leaving the system unattended.
2. Retain the device lock until the user reestablishes access using established identification and authentication procedures.
3. Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

**NOTE:** In the interest of safety, devices that are (1) part of a criminal justice conveyance (patrol vehicle) or (2) used to perform dispatch functions and located within a physically secure location, or (3) terminals designated solely for the purpose of receiving alert notifications (i.e., receive only terminals) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement.

09. SESSION TERMINATION

1. Ensure that the system automatically terminates a user session after a user has been logged out.

10. PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

1. Identify any specific user actions that can be performed on the system without identification or authentication consistent with organizational missions and business functions.
2. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

11. REMOTE ACCESS

1. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.
2. Authorize each type of remote access to the information system prior to allowing such connections.
3. Employ automated mechanisms to monitor and control remote access methods.
4. Ensure that the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
5. Ensure that the information system routes all remote accesses through authorized and managed network access control points to reduce the risk for external attacks.
6. Authorize the execution of privileged commands and access to security relevant information via remote access only in a format that provides accessible evidence and compelling operational needs.
7. Document the rationale for such access in the security plan for the information system.

12. WIRELESS ACCESS

1. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.
2. Authorize wireless access to the information system prior to allowing such connections.
3. Ensure that the information system protects wireless access to the system using authentication of authorized users and agency-controlled devices and encryption.
4. Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

13. ACCESS CONTROL FOR MOBILE DEVICES

1. Establish usage restrictions, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas.
2. Authorize the connection of mobile devices to organizational systems.
3. Employ full-device encryption to protect the confidentiality and integrity of information on full and limited-featured operating system mobile devices authorized to process, store, or transmit CJI.

14. USE OF EXTERNAL INFORMATION SYSTEMS

1. Establish agency-level policies governing the use of external systems consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:
2. Access the system from external systems.
3. Process, store, or transmit organization-controlled information using external information systems.
4. Prohibit the use of personally owned information systems including mobile devices (i.e., bring your own device (BYOD)) and publicly accessible systems for accessing, processing, storing, or transmitting CJI.
5. Permit authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:
6. Verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan.
7. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.
8. Restrict the use of organization controlled portable storage devices by authorized individuals on external systems.

15. INFORMATION SHARING

1. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information’s access and use restrictions as defined in an executed information exchange agreement, i.e., management control agreement, user agreement.
2. Employ attribute-based access control or manual processes as defined in information exchange agreements, i.e., management control agreements, user agreements, to assist users in making information sharing/collaboration decisions.

16. PUBLICLY ACCESSIBLE CONTENT

1. Designate individuals authorized to post information onto a publicly accessible information system.
2. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.
3. Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.
4. Review the content on the publicly accessible information system for nonpublic information quarterly and removes such information, if discovered.

PROCEDURES

Agency must provide the procedures on how the policies will be implemented.

COMPLIANCE

Agencies are required to review and update the current incident response policy and procedure annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

REFERENCE

AC-3, AT-2, AT-3.