Enterprise Technology Strategy and Services Policy 10-10
Access Control (AC)                                      Brian Tardiff, CISO
Last Revision: 8/28/2020                                doa.entsec@doit.ri.gov

1. Purpose

Establish policy for effective implementation and management of logical and physical access controls to safeguard State of Rhode Island IT system resources, infrastructure, and data. Controlling access to information systems and data is a fundamental function of information security. Access controls ensure that only authorized users access network resources they have been authorized to access and are critical in establishing user accountability for actions performed on systems.

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. Definitions

Access Privileges
Permissions and access rights of information system user accounts and/or processes required for accessing specific system resources and data.

Authentication
Establishing the validity of the user’s claimed identity using one or more of the following techniques: something the user knows (e.g. password), something the user has (e.g. key card), or something the user is (e.g. biometric fingerprint).

Federal Tax Information (FTI)
Federal tax returns and return information (and information derived from it) in the state agency’s possession or control covered by confidentiality protections of the Internal Revenue Code (IRC) and subject to IRC 6103(p)(4) safeguarding requirements, including Internal

\(^1\) State of Rhode Island Executive Branch Departments does not include the University of Rhode Island, the State Colleges, the General Treasurer, the Attorney General, or the Secretary of State.
Revenue Service (IRS) oversight. FTI includes return or return information received directly from IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or other entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(B) Agreement. FTI includes any information created by the recipient that is derived from federal return or return information received from IRS or obtained through a secondary source. Safeguarding FTI is critical to protecting taxpayer confidentiality as required by IRC 6103 and may not be masked to change the character of information to circumvent IRC 6103 confidentiality requirements.

Identification
Providing the user’s claimed identity to the information system, most commonly via a user ID.

Least Privilege
The principle that system users should be granted only the privileges required to perform their official duties and job functions.

Logical Access
The ability of a user to interact with hardware and data through access control procedures, such as identification, authentication, and authorization. For this policy, the term “access” refers to logical access.

Mobile Device
A computing device that is easily portable, has its own operating system, and is able to run application software. Typically, mobile devices have a display screen, a method to input data (e.g. touch screen, touch keyboard, miniature keyboard), and the ability to communicate and transfer data wirelessly (e.g. Wi-Fi, Bluetooth). Examples of mobile devices include, but are not limited to, tablets, laptops, notebooks, smartphones, and other portable computing devices.

Multifactor Authentication (MFA)
A method of authentication that requires at least two forms of independent credentials be verified prior to being granted access: something the user knows (e.g. password), something the user is (e.g. biometric), and/or something the user has (e.g. security token).

Personally Identifiable Information (PII)
Data, including FTI and SSA data, that can be used either alone or in combination with other data to identify an individual. Regardless whether in digital or hard copy paper format, data is considered PII when an individual's first name, or first initial and last name, in combination with one or more of the following data elements:
- Social Security Number (SSN)
- Driver's license number, RI identification card number, or tribal identification number
- Account, credit, or debit card number, in combination with any required security code, access code, password, or personal identification number that would permit access to an individual's financial account.
• Medical or health insurance information
• Email address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.

Physical Access
The ability to gain physical access to a computer or information system.

Privileged Account
An information system account that is granted an elevated level of privileges to access sensitive information systems and data, perform security related functions on the network, information system, or application, and provide for the management and configuration of mission-critical information systems and network infrastructure. Privileged accounts include, among others, local administrators, domain administrators, emergency accounts, service accounts, and application accounts.

Separation of Duties
The principle that roles and responsibilities should be divided among different users so that no single individual may subvert the information system or a critical business function.

Session
A series of interactions between two end points (e.g. desktop, server, web application, client/server) that occur during the span of a single connection.

Social Security Administration (SSA) Data
Data under the control of SSA provided to the state agency under the terms of an Information Exchange Agreement with the SSA, including data provided to the state agency by a source other than SSA but for which the state agency attests to that the SSA verified it or the state agency couples the data with other SSA data to certify its accuracy. SSA data includes:
• SSA’s response to a request from the state agency for information from SSA (e.g. date of death).
• SSA’s response to a query from the state agency for verification of an SSN.
• Display by the state agency of SSA’s response to a query for verification of an SSN and the associated SSN provided by SSA.
• Display by the state agency of SSA’s response to a query for verification of an SSN and the associated SSN provided to the state agency by a source other than SSA.
• Electronic records that contain only SSA’s response to a query for verification of an SSN and the associated SSN whether provided to the state agency by SSA or a source other than SSA.
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 system. At a minimum, any information system that stores, processes, transfers, or communicates PII or other sensitive data types is classified as a Moderate system.

4.1. [IAL1, IAL2] Access Control Policy and Procedures (AC-1). The agency will develop, document, disseminate, review, and annually update an access control policy and procedures.

4.2. [IAL1, IAL2] Account Management (AC-2). The agency will:
- Identify and select information system accounts to support agency mission and business functions. Privileged accounts will only be assigned to personnel that require elevated levels of access to perform their job functions.
- Assign account managers for information system accounts.
- Establish conditions for group and role membership.
- 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) are not authorized without prior written approval from the state CISO. An up-to-date record of all users authorized to access the information system will be maintained by the agency.
- Specify access privileges for each information system account. Access privileges assigned to external users will be commensurate with access restrictions of the respective agency information system. The agency will develop procedures for documenting and authorizing access privileges. A current record of granted access privileges will be maintained by the agency.
- Require approval from authorized personnel for requests to create information system accounts. Privileged users require approval from the system owner.
• Create, enable, modify, disable, and remove information system accounts in accordance with agency account management procedures. Inactive user accounts will be disabled after ninety (90) days of inactivity and, for privileged accounts, after sixty (60) days of inactivity. Where possible, this process should be automated by the information system.

• 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.

• Notify account managers 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 account manager will promptly submit a service ticket request that the system administrator modify or remove the account, as appropriate.

• 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.

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

• 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). The agency will employ automated mechanisms to support the management of information system accounts.

4.2.2. [IAL2] Removal of Temporary/Emergency Accounts (AC-2.2). The information system will automatically disable or remove, as appropriate, temporary and emergency accounts when they’re no longer required. The agency will identify the conditions and period of time when temporary and emergency accounts will automatically be disabled by the information system. In general, temporary and emergency accounts should be disabled immediately following the resolution of the issue that required their use.

4.2.3. [IAL2] Disable Inactive Accounts (AC-2.3). The information system will automatically disable inactive user accounts after ninety (90) days of inactivity and, for privileged accounts, after sixty (60) days of inactivity.

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.

4.3. [IAL1, IAL2] Access Enforcement (AC-3). The information system will (i) enforce approved authorizations for logical access to information and system resources, (ii) identify and authenticate each user prior to granting system access, (iii) maintain the identity of all active users, and (iv) link system actions to individual users. The authentication method
used will be commensurate with the sensitivity of the information system and data being accessed. For more information, see ETSS Enterprise Password Security Policy 10-01.

4.4. [IAL1, 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.

4.5. [IAL1, IAL2] Separation of Duties (AC-5). All aspects of access control enforcement will be performed in a manner consistent with the separation of duties principle. The agency will separate the duties of individuals, document separation of duties of individuals, and define information system access authorizations to support separation of duties. Agency policies, procedures, and standards that address agency-specific business needs and regulatory/compliance requirements, will be developed in accordance with the separation of duties principle to ensure the confidentiality, integrity, and availability of agency information systems and data.

4.6. [IAL1, 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. Privileged information system accounts will be restricted to individuals who require privileged access to perform their administrative duties. Privileged users should use non-privileged accounts when accessing non-security functions.

4.6.1. [IAL2] Authorize Access to Security Functions (AC-6.1). The agency will explicitly authorize access to security functions deployed in hardware, software, and firmware and security-relevant information.

4.6.2. [IAL2] Non-Privileged Access for Non-security Functions (AC-6.2). The agency will 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] Privileges Accounts (AC-6.5). The agency will restrict privileged accounts on the information system to designated personnel (or roles).

4.6.4. [IAL2] Auditing Use of Privileges Functions (AC-6.9). The information system will audit the execution of privileged functions, including the establishment of information system accounts, performance of system integrity checks, and the administration of cryptographic key management activities.

4.6.5. [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.

4.7. [IAL1, IAL2] Unsuccessful Logon Attempts (AC-7). The information system will automatically lock user accounts after three (3) consecutive invalid logon attempts. Locked non-privileged accounts will be locked for a minimum of ten (10) minutes before automatically unlocking. Locked privileged accounts will remain locked until unlocked by a system administrator.

4.8. [IAL1, IAL2] System Use Notification (AC-8). The information system will display a system use notification message (i.e. warning banner) on the screen at each login attempt prior to granting system access until the user acknowledges and explicitly agrees to the system use notification message. In general, the system use notification message should provide users with general policy on system use, prohibited activities, and privacy or security concerns.

Non-Public Information Systems
The information system will display a system use notification message prior to granting access that states (i) the user is accessing a State of Rhode Island government information system, (ii) system use is monitored, recorded, and subject to audit, (iii) use of the system implies user consent to being monitored and recorded, and (iv) unauthorized use of the system is prohibited and subject to criminal and civil penalties.

Publicly Accessible Information Systems
The information system will display a system use notification message prior to granting access that (i) displays system use conditions, (ii) references monitoring, recording, or auditing that are consistent with privacy accommodations for the system, and (iii) includes a description of the authorized uses of the system.

4.9. [IAL1, IAL2] Session Lock (AC-11). The information system will automatically prevent further access to the system by initiating a session lock after 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.

4.10. [IAL1, IAL2] Session Termination (AC-12). The information system will automatically terminate user-initiated sessions after 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). No actions will be performed on any information system that is not publicly accessible without user identification and authentication. For publicly accessible information systems, only public content (i.e. public data) may be accessed without the user being identified.

4.12. \[IAL1, IAL2\] Remote Access (AC-17). The agency will authorize remote access to agency information systems via an external network (e.g. internet) prior to granting such connections and establish/document usage restrictions, configuration and connection requirements, and implementation guidance for each type of remote access method allowed (e.g. broadband, VPN). Mechanisms that provide remote access to information systems will be managed and maintained by ETSS. MFA will be required for all remote access to the state network and information systems.

4.12.1. \[IAL2\] Automated Monitoring/Control (AC-17.1). The information system will 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. \[IAL2\] Managed Access Control Points (AC-17.3). The information system will route all remote accesses through a limited number of managed network access control points (e.g. firewalls, routers, switches). Access control points will be managed and maintained by ETSS.

4.12.3. \[IAL2\] Privileged Commands/Access (AC-17.4). The agency will authorize, and document within the system security plan, the execution of privileged commands and access to security-relevant information via remote access.

4.13. \[IAL1, IAL2\] Wireless Access (AC-18). The agency will (i) establish usage restrictions, configuration and connection requirements, and implementation guidance for wireless access and (ii) authorize wireless access to the information system prior to allowing wireless connections. Mechanisms that provide wireless access to the state network will be managed and maintained by ETSS. See ETSS Wireless Access Policy 04-02 for more information.

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. See ETSS Wireless Access Policy 04-02 for more information.

4.14. **[IAL1, IAL2]** Access Control for Mobile Devices (AC-19). The agency will (i) establish usage restrictions, configuration requirements, and connection requirements for agency controlled mobile devices and (ii) authorize the connection of mobile devices to agency information systems. See ETSS Mobile Device Security Policy 10-04 for more information.

4.14.1. **[IAL2]** Full Device/Container-Based Encryption (AC-19.5). The agency will employ encryption to protect the integrity and confidentiality of information on mobile devices. All state-owned mobile device will be encrypted. Any exception to this requirement requires formal approval by the state CISO. See ETSS Mobile Device Security Policy 10-04 for more information.

**[IAL1, IAL2]** Use of External Information 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. personally owned computers and smartphones, infrastructure/software/platform as a service cloud services). The agency will establish terms and conditions under which authorized users can (i) access non-public interfaces of agency information systems from external information systems and (ii) process, store, or transmit agency data using external information systems. External information systems must meet security control standards required by the agency and ETSS. The agency should identify, at a minimum, applications on agency information systems that can be accessed from external information systems and the types of agency data (e.g. private, sensitive) that external information systems can process, store, or transmit. Terms and conditions include applications that can be accessed on agency information systems from external systems, as well as the strictest security category of information that can be processed, stored, or transmitted on external systems.

4.14.2. **[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 (i) verifies that required security controls are implemented on external information systems and (ii) maintains approved information system connection or processing agreements with the organization hosting the external information system. Depending on the confidence level required, verification can be achieved via third-party reviews, independent assessments, or other attestation.

4.14.3. **[IAL2]** Portable Storage Devices (AC-20.2). The agency will restrict the use of agency-controlled portable devices on external information systems.

4.15. **[IAL2]** Information Sharing (AC-21). The agency will restrict the sharing of information (e.g. medical, contract, proprietary, PI, or other sensitive or controlled information) 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 discretion is required.

4.16. [IAL1, IAL2] Publicly Accessible Content (AC-22). The agency will (i) designate and train individuals authorized to post information on a publicly accessible information system, (ii) review the information prior to posting onto a publicly accessible information system to ensure only public information is included, and (iii) annually review content posted on publicly accessible information systems for non-public data and, if discovered, remove such information.

5. Approval / Review Signature:

Brian Tardiff
Digitally signed by Brian Tardiff
Date: 2020.09.14 08:52:05 -04'00'

Chief Information Security Officer