	Department of Human Services Online Directives Information System	**Index:** **Revised:** **Next Review:**	**POL1901** **08/30/2019** **08/30/2021**

SUBJECT: DHS Information Security

Policies Access Control Policy

POLICY

To establish and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components that limit access to information assets to only those individuals that are authorized to obtain it. The objective of this policy is to address the considerations that will help to ensure that the DHS IT resources and information systems are properly protected against unauthorized access, while meeting the access requirements for all authorized users. Critical to achieving this objective is the implementation of controls that address each of the requirements stated in this policy.

Authority

1. United States Department of Commerce National Institute for Standards and Technology (NIST)
2. United States Internal Revenue Service
3. United States Department of Health & Human Services
4. Centers for Medicare & Medicaid Services
5. Georgia Technology Authority

References

- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, January 2015
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-100 “Information Security Handbook: A Guide for Managers” March 2007
- Federal Information Security Management Act of 2002 (FISMA)
- Georgia Technology Authority Enterprise Information Security Policy
- United States Internal Revenue Service, IRS Publication 1075 Tax Information Security Guidelines For Federal, State and Local Agencies Safeguards for Protecting Federal Tax Returns and Return Information
- Centers for Medicare & Medicaid Services, Volume II: Minimum Acceptable Risk Standards for Exchanges

Applicability

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by DHS. Any information not specifically identified as the property of other parties, that is transmitted or stored on DHS IT resources (including e-mail, messages and files) is the property of DHS. All users (DHS employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

Definitions

Access Control - Access control is way of limiting access to a system or to physical or virtual resources. In computing, access control is a process by which users are granted access and certain privileges to systems, resources or information.

Least Privilege - is the practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, the principle of least privilege translates to giving people the lowest level of user rights that they can have and still do their jobs.

Role-based Access Control (RBAC) - is a method of access security that is based on a person's role within a business or group.

Sensitive Data – information that is protected against unwarranted disclosure and requires specific safeguarding requirements. Sensitive data includes, but is not limited to, Federal Tax Information (FTI), Social Security Administration verified/provided information, Personally Identifiable Information (PII), Personal Health Information (PHI), etc.

Responsibilities

DHS shall adopt the Access Control principles established in NIST SP 800-53 "Access Control," Control Family guidelines, as the official policy for this domain. The following subsections outline the Access Control standards that constitute this policy. Each DHS Business System is bound to this policy and shall develop or adhere to a program plan which demonstrates compliance with the policy related to the standards documented.

- **AC-1 Access Control Policy and Procedures**
    1. Senior management, management, and all organization entities are required to coordinate and implement necessary controls for providing authorized access and preventing unauthorized access to IT resources and information systems on the basis of business and security requirements.
    2. Periodic reviews of this policy shall be performed and documented at least within every **three years**, or when there is a **significant change**.
    3. Periodic review of access control procedures shall be performed at least **annually**.

- **AC-2 Account Management**
    1. Manage through a life cycle consisting of establishing, activating and modifying accounts; periodically reviewing accounts; and disabling, removing or terminating information system accounts, defined as individual, group, system and role-based accounts defined as administrator, application, guest and temporary.
    2. Users who require access to FTI data shall be assigned to agency specific account types with access to Federal Tax Information (FTI) to support agency missions/business functions.
    3. Conditions for user assignment to group membership shall be established and maintained.
    4. Document within applicable system security plans a description of authorized system users criteria group and role accounts' membership with access privileges, and other applicable account attributes.
    5. Require System Administrators, Account Managers, managers and supervisors to adhere to the following requirements regarding creating, enabling, modifying, disabling or removing accounts:
        a) Valid access authorization,
        b) Intended system usage,
        c) Specific attributes required by the organization or associate mission/business functions.
    6. Users must obtain appropriate approvals for requests to establish accounts, to include, but not limited to, supervisor approval, management approval, and agency approval.
    7. Agency IT administrators shall establish, activate, modify, disable, and remove accounts in accordance with documented account management procedures.
    8. Explicit authorization and monitoring of the use of temporary accounts. The use of guest/anonymous accounts is prohibited.
    9. Agency users are responsible for immediately notifying account managers when:
        a) Temporary accounts are no longer required,
        b) When information system users are terminated, transferred,
        c) Information system usage or need-to-know/need-to-share changes.
    10. The agency explicitly authorizes access to information systems that receive, process, store, or transmit FTI based on a valid access authorization, need-to-know permission, and under the authority to re-disclose FTI under the provisions of IRC 6103.
    11. Accounts shall be reviewed periodically or at **least annually** to ensure compliance with account management requirements. Shared/Group

account credentials shall be established or reissued in accordance with established account management procedures.

12. Information Systems that host, store and transmit FTI shall be automatically disabled and de-provisioned after **120 days of inactivity**

- **AC-3 Access Enforcement**
    1. The agency shall employ formal registration and de-registration procedures for granting and revoking access to all information systems and services, in accordance with applicable policy.
    2. Established role-based access controls (RBAC) for employee user accounts requiring access to information systems and data that contain FTI upon authorization shall be employed exercised.
- **AC-4 Information Flow Enforcement**

  Explicitly approved authorizations for controlling the flow of FTI information within the system and between interconnected systems shall be maintained in accordance with applicable policy and the technical safeguards in place to protect FTI.
- **AC-5 Separation of Duties**
    1. The agency separates duties of individuals as necessary, to prevent malevolent activity without collusion.
    2. Documented separation of duties shall be maintained.
    3. Implement separation of duties through assigned information system access authorizations shall be employed and maintained.
- **AC-6 Least Privilege**
    1. The agency continuously utilizes the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
    2. Access to FTI must be explicitly authorized prior to individuals gaining access to FTI.
    3. Access to FTI by contractors is prohibit, unless authorized by the IRS Office of Safeguards, as identified in IRS Publication 1075.
    4. Users of information system accounts, roles, with access to FTI, are required to use non- privileged accounts or roles when accessing non-security functions.
    5. Role-based account assignment and usage is required to restrict user access, privilege accounts to privileges necessary to accomplished assigned tasks.

- **AC-7 Unsuccessful Login Attempts**
    1. Automatic lockout mechanisms for information systems that host, store and

transmit FTI data when the maximum number of unsuccessful attempts are exceeded is enforced.

2. Repeated access attempts by locking out the user ID is limited to **no more than three consecutive** unsuccessful attempts during a **120 minute period**.
3. Automatically lock the account for a period of **at least 15 minutes**.

- **AC-8 System Use Notification**
    1. Agency information systems display an approved system use notification banner before granting access to the system. This banner provides privacy and security notices consistent with regulations, standards, and policies. The system use notification shall state:
        a) The system contains U.S. Government information
        b) User actions are monitored and audited
        c) Unauthorized use of the system is prohibited
        d) Unauthorized use of the system is subject to criminal and civil sanctions
    2. The notification banner remains on the screen of agency information systems until users take explicit actions to log on to or further access the information system.
    3. For publicly accessible systems:
        a) The IRS-approved warning banner is displayed on the information system screen prior to granting further access
        b) The display references the consent to monitoring, recording, or auditing on the information system
        c) A description of the authorized uses for the information system are displayed
- **AC-11 Session Lock**
    1. Further access to the information system is prohibited by the initiation of a session lock after **15 minutes of inactivity** or upon receiving a request from a user.
    2. The session lock is maintained until the user reestablishes access using established identification and authentication methods.
- **AC-12 Session Termination**
  DHS shall enforce the automatic termination of user sessions after **30 minutes of inactivity**.
- **AC-14 Permitted Actions without Identification or Authentication**
    1. The agency does not permit actions within agency information systems without proper identification and authentication. Sensitive data disclosure is prohibited to individuals on the information system without identification and authorization.
    2. Documentation and rationale supporting the decision to deny actions on

information systems without identification and authentication is documented and maintained in the agency's SSRs.

- **AC-17 Remote Access**
    1. Remote access to agency information systems is authorized only through the use of established VPN. If remote transmission of sensitive data is required, it shall only be transferred through the use of VPN, and shall utilize multi-factor authentication.
    2. FTI access offshores (outside of the United States territories, embassies or military installations) is prohibited by agency employees, agents, representatives, or contractors.
    3. Sensitive data may not be received, processed, stored, transmitted, or disposed of by information technology (IT) systems located offshore (outside of the United States territories, embassies or military installations).
    4. Users requiring remote access have been assigned VPN accounts which facilitate remote access to agency information systems. VPN traffic is routed through a limited number of managed network access points, such that authorized personnel shall only have access to the information systems or services required to perform their job functions.
    5. Privileged commands and access to security-relevant information via remote access must be explicitly approved by management and documented prior to performing those functions. Authorization shall only be granted under compelling operational needs.
- **AC-18 Wireless Access**
    1. DHS capabilities for wireless access are limited to only establish connections to guest networks only.
    2. Access to agency internal information systems and data via wireless is prohibited.
    3. Access to sensitive data via wireless is prohibited.
- **AC-19 Access Control for Mobile Devices**
    1. Only agency provided mobile devices are authorized for connection and use within the agency's network/information systems.
    2. Mobile devices authorized for use within the agency's network/information system must utilize encryption in order to protect the confidentiality and integrity of information on authorized mobile devices.
    3. After **10 consecutive, unsuccessful device logon attempts,** mobile devices shall be purged/wiped. (Laptop computers are excluded from this requirement.)
- **AC-20 Use of External Information Systems**
    1. Unless approved by the IRS Office of Safeguards, Social Security

Administration, or other applicable governing entities, the following are strictly prohibited:

a) Access to FTI from external information systems other than through a virtual desktop infrastructure,
b) Using agency-controlled portable storage devices containing sensitive data on external information systems,
c) Using non-agency owned or controlled information systems, components, or devices to process, store, or transmit sensitive data. Any non-agency owned information system usage requires the agency to submit notification to the Office of Safeguards 45 days prior to implementation.

- **AC-21 Information Sharing**
  1. The sharing/re-disclosure of FTI is restricted only to personnel authorized in IRC 6103, and as approved by the IRS Office of Safeguards.
  2. The sharing/re-disclosure of other sensitive data is restricted to personnel authorized in contractual agreements and approved by that governing entity.
- **AC-22 Publicly Accessible Content**
  1. Only agency authorized personnel shall post information onto an organizational information system that is publicly accessible. Agency/organizational units shall maintain listings of authorized personnel.
  2. All personnel identified in the authorized list shall receive training to ensure that publicly accessible information does not contain sensitive data.
  3. Content that shall be posted to publicly accessible information to ensure it contains no sensitive data information prior to posting.
  4. If publicly accessible information is found to have sensitive data information, authorized personnel shall remove it immediately.

History
None

Evaluation
The Office of Information Technology (OIT), upon recommendation of the DHS Chief Information Security Officer (CISO), evaluates this policy annually by:

1. Comparing its content and intent to evolving regulatory compliance standards imposed upon the Agency, such as, IRS 1075, NIST 800-53, and CMS MARS-E.
2. Addressing any deficiencies or gaps discovered during periodic audits conducted by Georgia DOAA or other regulatory bodies, such as, IRS, CMS, SSA, FBI, etc.