Health Services LOS ANGELES COUNTY Information Technology	
DHS SYSTEM ACCESS CONTROL POLICY	**POLICY NUMBER** 167 **VERSION NUMBER** 1
REVIEW CYCLE ☐ 1 year ☐ 2 years ☒ 3 years **EFFECTIVE DATE:** 12/28/2024 **LAST REVIEW DATE:** 12/28/2024 **NEXT REVIEW DATE:** 12/28/2027	**ATTACHMENTS** ☐ YES ☒ NO

PURPOSE

To preserve and protect the confidentiality, integrity, and availability of the Department of Health Services (DHS) networks, systems and applications, all access to the Information Technology Assets/Resources are permitted only to those persons or software programs that have been granted appropriate access rights.

POLICY STATEMENT

DHS Facility CIOs/designees must ensure that DHS facility System Managers/Owners implement the appropriate technical access control safeguards to allow DHS electronic information systems access only to those persons or software programs that have access clearance or have been granted access rights with a level of privilege that allows them to only access the minimum information for which they are authorized.

DEFINITIONS

For a more complete definition of terms used in this policy and/or procedure, see the DHS Information Security Glossary (Attachment I) to DHS Information Technology and Security Policy.

PROCEDURES

DHS System managers/owners must ensure appropriate technical safeguards are implemented to allow access to authorized users and that access is granted only to information that is minimally necessary to accomplish the intended purpose of the use, disclosure, or request (need to know).

I. **Granting and Revoking Access:** For granting and revoking access, refer to the DHS Workforce Security Policy.

II. **Unique User Identification (ID):** DHS System managers/owners must ensure that DHS systems assign a unique name and/or number to uniquely identify and

track each workforce member's activities and regulate who may view or access what resources in DHS' managed networks, systems, and applications that may contain Protected Health Information (PHI) as required by the DHS System Audit Controls Policy.

A. Any workforce member who requires access to any network, system, or application that creates, accesses, transmits, receives, or stores EPHI, must be provided with a unique user ID string.
    a. System managers/owners must clearly define the naming/numbering format for system users.
    b. The system must be able to identify the unique username and allow audit capabilities in accordance with the recommended safeguards specified in the DHS System Audit Controls Policy.
B. Each workforce member must ensure that their assigned User ID and password is protected appropriately and only used for legitimate access to networks, systems, or applications.
    a. If a workforce member believes their user ID and/or password has been compromised, the individual must report it immediately in accordance with the DHS Security Incident Report and Response Policy.
C. Any workforce member who suspects their password may be compromised or is known by someone must immediately change their password and report the incident to DHS Enterprise Help Desk and their management.
D. Workforce members' passwords must follow the requirements specified in the DHS Workstation and Mobile Device Use and Security Policy.
E. Each workforce member must protect his/her password. They must not write down their password and place it at or near the workstation (e.g., a note taped to the monitor or placed under the keyboard).
F. Logging into workstations, networks, or applications with another user's ID and/or password is prohibited. It is prohibited to ask to share a password.
G. Workforce members must not share their unique User IDs and passwords with any other person including management and IT support personnel.

III. **Multi-factor authentication:** To protect DHS systems and confidential information from external threats, system managers/owners must ensure that workforce members who require remote access, provide two or more means of identification, one of which is typically physical (e.g., registered device, phone number, text number, a one-time code via a registered mobile application), and the other of which is typically something memorized (e.g., a secret Personal Identification Number (PIN)) is required for all critical systems, and for all resources being accessed remotely from outside DHS Network. This will

minimize the risk of hackers accessing DHS systems, should they succeed in phishing or guessing workforce members' login passwords.

IV. System Login Banner: DHS System managers/owners must ensure that every login process for multi-user computers includes a special notice. Any system connected/connecting to DHS network must display a system login banner with verbiage regarding authorized and acceptable use of a computer system and its resources, data, and network access capabilities at the point of access which sets the right expectations for everyone attempting to access such system. The notice must state:

A. The system is to be used only by authorized users, and

B. By continuing to use the system, the user represents that he/she is an authorized user.

V. System Log-in Monitoring: DHS System managers/owners must ensure that users' activities and the process for accessing systems is recorded and monitored for successful and failed attempts. Such monitoring allows the DHS Information Security Office to identify suspicious activities, and systematic unauthorized penetration attempts by malicious hackers targeting DHS computing devices, systems, or network and react in real time to interrupt and block such explorations in order to avoid any data compromises that can result in data compromises or breach of information. DHS system owners/managers must enable access logging by users or processes. Logs should include attributes such as "When", "Where", "Who", "What", and "How" for each event initiated by the system's application and user for both information at rest (storage) and information in transit (transmission). Detailed specifications can be found in the DHS System Audit Controls Policy.

VI. Emergency Access Procedure: DHS System managers/owners must ensure that DHS systems have alternate secured manual or automated procedures for accessing stored information during an emergency to be invoked by the DISO or designee when the usual means of secured access is not available. Refer to the DHS Facility Information Technology Contingency Plan Policy.

VII. Automatic Logoff: DHS Facility CIOs/designees must ensure that the DHS facility System Managers/Owners address the use of an automated process to terminate an electronic session after a predetermined time of inactivity.

VIII. Encryption/Decryption: DHS Facility CIOs/designees must ensure that DHS facility System Managers/Owners address the appropriate encryption for protecting electronic information contained within the storage structure for all DHS electronic data storage systems (i.e., databases or file systems) and during

electronic or in-person transfers and transports. To minimize the possibility of sensitive or confidential data being compromised, encryption must be applied as follows:

A. Stored confidential data (at rest), having a Sensitivity Score of "High" (e.g., patient information), must be encrypted, or must be stored on a DHS approved secure network drive.

B. All electronic transfers and transportations for sensitive or confidential data must be encrypted.

C. All web sessions and web connections that include access or process of sensitive or confidential data must be secured by encryption.

D. Removable media containing confidential data (e.g., patient information) must be encrypted and stored in secure areas.

E. All workstations, desktop computers, laptops, notebooks, tablets, and portable devices containing sensitive information (e.g., confidential patient information) must be encrypted.

To minimize risks of incidental disclosures, workforce members must redact or delete files containing sensitive information within the storage structure for all DHS electronic data storage systems and folders once the business need has been satisfied and the documentation has been completed.

For further details on encryption, refer to the DHS Workstation and Mobile Device Use and Security Policy.

IX. Information System Access Control: Facility CIOs/designees, taking into consideration each system's Risk Analysis Sensitivity Score, must design and implement security controls to limit unauthorized access of workforce members to information systems including workstations, servers, networks, and applications.

X. System Security Documentation: DHS facility System Managers/Owners must document the implementation of the above safeguards in the System Security Implementation Plan that accompanies the electronic data system. The System Security Implementation Plan and all system documentation must be submitted to the Facility Information Security Officer (FISO) or designee for review.

REFERENCES

45 Code of Federal Regulations, Part 164, Subpart C, Section 164.308 (a)(3)(ii)

Board of Supervisors Policies:
6.100, Information Security Policy

6.101, Use of County Information Assets
6.102, Endpoint Security Policy
6.103, Information Security Incident Reporting and Response
6.105, Information Technology Audit and Risk Assessment

DHS Policies:
DHS Information Security Risk Management
DHS Facility Information Technology Contingency Plan
DHS System Audit Controls
DHS Data Security Documentation Requirement