**County of Los Angeles** **Department of Health Services**

# OLIVE VIEW-UCLA MEDICAL CENTER
# INFORMATION SYSTEM TECHNOLOGY OPERATIONS
# POLICY & PROCEDURE

**NUMBER: 11529**
**VERSION: 1**

**SUBJECT/TITLE: OVMC IT PROHIBITING ACCESSS TO SECURITY SENSITIVE SYSTEMS, AREAS AND NETWORKS POLICY**

| | |
|---|---|
| **POLICY:** | It is the Department's policy to ensure the security of all security sensitive systems. Managers/supervisors are responsible for assigning and determining appropriate access rights to security-sensitive systems and requesting immediate termination of such access, as appropriate. Managers/supervisors are required to immediately contact the system managers/owners of any security-sensitive system, area or network containing confidential and/or medical information when a workforce member has:<br>• Terminated from County service or assignment (voluntarily or involuntarily)<br>• Transferred from the facility or from the Department<br>• Been suspended from duty<br>• Been reassigned for administrative purposes where access is precluded or no longer required<br>• Performance/behavioral problems with respect to use of information technology and/or confidential records access<br><br>Particularly, access must be immediately restricted to pharmaceutical dispensing systems if the workforce member:<br>• Failed competency associated with medication administration/management<br>• Has performance/behavioral problems inclusive of possession of drugs/illegal drug usage<br>• Is suspected of diverting drugs from intended patient<br>• Is reassigned for administrative purposes where access is precluded or no longer required<br><br>The above is not an all-inclusive list of circumstances. Access must be immediately restricted but no later than close of the same business day or end of the workforce member’s shift. Managers/supervisors must use discretion and good judgment to ensure the security of security-sensitive systems, areas, and/or confidential records and the safety of workforce members and patients.<br><br>Assignment of access rights and request for termination shall be provided to the appropriate system/manager owner in writing, or in accordance with system policies and procedures. |

Managers/supervisors must immediately contact DHS Human Resources, Regulatory Compliance Informatics when a non-County workforce member's assignment in involuntarily terminated or the non-County workforce member has transferred to another facility.

Managers/supervisors are also responsible for immediately updating the non-County staff database (EHS) by entering the Assignment End Date for a terminated or "inactive" non-county workforce member.

Note: Managers/supervisors must notify Pharmacy, Information Technology (IT), etc. of the start and end dates of a non-County workforce members assigned (e.g. traveler, resident for non-DHS/non-DHS affiliated program).

DHS Human Resources, Information Systems will provide a personnel outgoing and leave management report to all system managers/owners on a weekly basis to assist system managers/owners with updating and restricting system access to workforce members.

DHS Human Resources, Regulatory Compliance, Informatics will provide system managers/owners with a quarterly report of the non-County workforce members who have terminated assignments. They will also provide periodic reports of non-County workforce members who have been placed in the "Do Not Send" database.

System managers/owners are responsible for immediately deleting access to their system in accordance with the outgoing reports and by manager/supervisor request. System managers/owners may refer to the DHS Policy 935.03, Workforce Security for guidance.

**PURPOSE:**

To ensure access to security-sensitive systems (e.g., pharmaceutical dispensing systems, medical and confidential information systems), medical and other confidential records, and facility secure areas is restricted from workforce members who have terminated from County service or assignment, transferred between facilities or out of the Department of Health Services (OHS), have been suspended, who are in an "inactive" status, or who have been restricted from certain aspects of their job responsibilities.

**DEPARTMENTS:**

**Information Systems – Technology Operations**

**REFERENCES:**

DHS Policy 935.03 (Workforce Security)
DHS Policy 935.031 (Prohibiting Access to Security-Sensitive Systems, Areas and Networks

**PROCEDURE:**

(SEE USER ACCOUNT AUDIT FOR NON-LDAP COMPLAINT SYSTEMS

| | PROCEDURE |
|---|---|
| | |

| | |
|---|---|
| References: | |
| Approved by: Chien-Ju Wang (Information Systems Specialist I) | Date: 06/14/2018 |
| Review Date: 06/14/2018 | Revision Date: |
| Next Review Date: Not Set | |
| Distribution: Information Systems | |
| Original Date: 06/14/2018 | |