Security Procedure

Policy: See N-04 LAN Accounts – Management and Use at www.cosdcompliance.org

Definitions: See HHSA Policy N-13 Security Definitions

Procedures:

A. LAN Account Requests

1. New LAN accounts are to be requested via the CSRF process and submitted with proof of the authorized user's background clearance.
    - County employees must complete privacy and security awareness training within 30 days of initial LAN account login.
    - Non-County users must sign the County Summary of Policies and include it with the CSRF request.
2. A LAN account is uniquely assigned to each authorized user and granted the minimum necessary of access based on the need to know.

B. User Responsibilities

1. The user must take all reasonable care to protect their account from being shared with anyone or used by someone else as the user is held responsible for all activity traced to their account.
    - If the account is compromised or suspected to be compromised, change the LAN account password immediately and report the incident to your manager/supervisor.

2. Users must not attempt to access any data or programs contained on the County's systems for which their LAN account does not have authorization or explicit consent.

3. Remotely accessing the LAN account such as from a home based computer must adhere to all the same policies that apply to use from within a County facility.

C. LAN Account Management:

1. LAN accounts for users on extended leave beyond 60 days must be disabled. Submit a CSRF 'Leave of Absence – Start' that disables the account to protect it during the user's absence. When the user's return date is known, submit another CSRF 'Leave of Absence – Return' to re-enable the LAN account.

2. All new LAN accounts that have not been accessed beyond 60 days of creation must be re-evaluated by the CSRF Authorizer to either disable it to maintain it or delete it if it is no longer needed.

3. Temporary County employees (e.g. Temporary Expert Professional, retired re-hirees) must have an expired date set on their LAN account not to exceed their service term or 12 months, whichever is less. CSRF Authorizers must re-certify the account to extend the expired date another 12 months or less.

4. LAN accounts have a home directory (H:\drive) associated with them. An H:\Drive will follow the user with transfers within the Agency. However, if the user transfers to another County Group (e.g. LUEG), the H:\Drive will not follow the user as HHSA remains as the custodian. The user will instead be assigned a new home directory in the other County Group. If a copy of the HHSA H:\Drive is needed, then a memo of approval from the user's last HHSA manager/supervisor will be required. Contact the Agency Compliance Office for assistance.

5. LAN accounts requested to be 'Terminated' will be placed in 'disabled' status and then be permanently removed from the system after 180 days.
    - The home directory associated with the LAN account will also be placed in 'disabled' status and then be permanently deleted from the system after 180 days. It cannot be restored.

D. <u>LAN Account Monitoring</u>:

1. Managers/supervisors are responsible to report, in a timely manner, relevant changes in user employment status and access requirements to the appropriate CSRF Authorizer in order to submit the CSRF promptly to make the change.
    - For 'transfer out' or 'terminations', a CSRF must be submitted at least two (2) days prior to the user's last day to allow processing time for the access and/or LAN account to be removed or deleted by the last day.
2. LAN Accounts in 'Enabled' status and that have been inactive beyond 60 days must be re-evaluated by the CSRF Authorizer to either disable it to maintain it or delete it if it is no longer needed.

3. LAN Accounts set to expire are to be re-evaluated one month in advance of the expired date by the CSRF Authorizer and is to submit a CSRF at least six (6) days prior to the expired date to either extend the expired date or delete it if it is no longer needed.
    - LAN accounts in 'expired' status beyond 60 days must be deleted unless a business justification exists to maintain the account.

E. <u>LAN Account Safeguards</u>

LAN Accounts shall be set up with the following security controls:

- LAN accounts must force a password change at initial login or password reset.
- LAN accounts must have passwords set to expire every 90 days.
- LAN accounts must lock after 15 minutes of inactivity.
- LAN account IDs must be unique to an individual
- LAN accounts must 'lock' to deny access after five consecutive invalid login attempts. The user must be verified to reset the password.

N – 04: LAN Accounts – Management and Use

F. LAN Accounts for Non-County Authorized Users:

1. An Agreement (e.g. contract agreement, MOA/MOU, license agreement) with the County must be in effect before a LAN account can be requested for the non-County Agency staff.
    - The County sponsor shall be responsible for submitting CSRF requests in a timely manner to create, terminate or re-certify non-County LAN accounts and of the level of access granted.

2. LAN accounts pertaining to Non-County users (e.g. volunteers, contractors, vendors, temp agency staff, State auditors) must be set to expire every 12 months or by the contract service end-date, whichever is less. The County sponsor must re-certify the account in a timely manner to extend the expired date another term and to prevent a gap in access.

3. Non-County users are allowed remote access only when they are assigned County equipment and/or are members of a specific SSLVPN2 group.

4. Proof of background clearance is not required for State of California employees (e.g. Auditors) to create a LAN Account. However, they must still sign the County Summary of Policies and be included with the CSRF request.

G. Emergency Access

Access to EPHI must be maintained or made immediately available to any caregiver during an emergency situation if the denial or strict access to that EPHI could inhibit or negatively affect patient care/treatment. Contact the appropriate system administrator for access to the needed electronic medical record.

Violations or suspected violations of this policy will be referred to the Agency Human Resources for appropriate personnel action or investigation.

QUESTIONS/INFORMATION: HHSA Information Security Manager at 619-338-2634