SLDCADA Role Responsibilities, and Security-Related Responsibilities

SLDCADA

I have read and understand the descriptions of the roles and responsibilities and security policy information contained within the attached document. I acknowledge and agree to use all SLDCADA's systems in accordance with the terms outlined in this document. I understand that failure to comply with these policies may result in revocation of my access to SLDCADA online records systems, adverse action, and/or civil or criminal liability under applicable laws.

_____
Signature

_____
Name (Printed)

_____
Organization

_____
Date

Your Role

Self-User ☐
Timekeeper ☐
Certifier ☐
Customer Service Representative ☐
SLDCADA Site Administrator ☐

User Contact Information

SLDCADA User ID: _____
Instance Name: _____
Phone Number: _____
Email Address: _____

SLDCADA

SLDCADA Role Responsibilities, and Security-Related Responsibilities

1. Laws and Policies Governing Protection of Personal Information

1.1. Public Law 93-579, U.S.C § 552a

- Privacy Act of 1974
  - Virtually all data within SLDCADA contains sensitive but unclassified (SBU) information that is subject to protection from disclosure under the Privacy Act of 1974.
  - Examples of privacy information not releasable to public:
    - Date of birth
    - Home address
    - Home telephone no.
    - Home e-mail
    - Net salary
    - Deductions
    - Debts
    - Leave balance
  - SLDCADA accounts are issued for the performance of official duties only. Any other use is strictly prohibited.
  - Users cannot certify their own records.

1.2. Freedom of Information Act

- Enacted in 1966 to provide universal access to official information
- Categories that are exempt from FOIA:
  - Classified information
  - Internal rules and practices
  - Information denied by other specific withholding statutes
  - Trade secrets and commercial or financial information given in confidence
  - Intra- and interagency communication
  - Personal information protected by the Privacy Act
  - Investigative information compiled for law enforcement
  - Reports on financial institutions

1.3. PKI Policy

- DOD requires that private Web servers enforce PKI on 1 April 2004.
- DOD employees and their contractors need either soft certificates (on a floppy) or CAC.
- All DoN commands and personnel obtain CAC-based PKI certificates
  - Sign and encrypt e-mail
  - Access to private Web servers
  - Cryptographic based network logon
  - Includes military, civilian, and eligible contractors

2. User Responsibilities

- Safeguard sensitive but unclassified (SBU) and Privacy Act data
- Log off when finished
- Protect the computer screen from casual observers

- Destroy reports (shredding or burning)
- Secure reports in an NSA-approved container
- Don't share information with anyone who doesn't have a need to know

2.1. Terminal User Responsibility

- Protect your password; do NOT write it down and do NOT divulge it to anyone.
- Use only the user ID and password you were assigned.
- Protect your keyboard and screen while entering your password.
- Do not leave your terminal unattended while logged into SLDCADA. Instead, log off or lock your terminal.
- You are responsible for protecting and maintaining any information used or stored in your accounts, to the best of your ability.

3. Agencies' policies control Time and Attendance (T&A), ensuring that data:

- Is recorded promptly, completely, and accurately
- Reflects actual work performed and leave taken
- Is sufficiently detailed to allow certification
- Complies with legal requirements
- Is supported by recorded evidence of supervisor review and approval

4. Roles and Responsibilities

Integrity of T&A recorded depends on conscious oversight of supervisors, timekeepers, certifiers, or other approving authority. Below are listed some of the default roles used in the SLDCADA application and role-related responsibilities.

4.1. Self-User Responsibilities

- Record T&A and review to ensure accuracy and completeness prior to certification.
- T&A should be approved at the end of the last day of the pay period or later.
- Notify Certifier when T&A is available for certification.
- Generate SLDCADA reports:
    - Incorrect Hours

4.2. Timekeeper Responsibilities

- T&A should be approved at the end of the last day of the pay period or later.
- Official most knowledgeable of time worked should approve overtime and/or clocks.
- Record work schedule, shift, and predetermined JON changes.
- Record T&A and review to ensure accuracy and completeness prior to certification.
- Notify Certifier when T&A is available for certification.
- Enter prior pay adjustments.
- Notify Certifier when prior pay is available for certification.
- Generate SLDCADA reports:
    - Incorrect Hours
    - Unsent Prior Pay Corrections (v22: Pending Prior Pay Corrections)

SLDCADA

4.3. Certifier Responsibilities

- Review time for assigned employees to ensure accuracy.
- Correct incorrect time or refer to employee/ Timekeeper.
- Certify time.
- Enter/certify prior pays.
- Maintain Primary/Alternate Timekeepers and Alternate Supervisors.
- Generate SLDCADA reports:
    - Incorrect Hours
    - Unsent Prior Pay Corrections (v22: Pending Prior Pay Corrections)
    - Uncertified Employees

4.4. Customer Service Representative Responsibilities

- Maintain employee data (e.g., shop and supervisor assignment).
- Coordinate with SLDCADA Administrator to grant user access.
- Maintain work schedule codes.
- Maintain SLDCADA validation tables.
- Monitor input of T&A.
- Generate SLDCADA Reports:
    - Centralized:
        - Incorrect Hours
        - Civilian Employee Additions (v22: Employee Additions)
        - Civilian Employee Changes (v22: Employee Changes)
        - Civilian Employee Deletions (v22: Employee Deletions)
        - Civilian MER Load Errors (v22: Error/Batch Employee Messages)
    - Decentralized:
        - Incorrect Hours
        - Uncertified Employees
        - Civilian Employee Additions (v22: Employee Additions)
        - Civilian Employee Changes (v22: Employee Changes)
        - Civilian Employee Deletions (v22: Employee Deletions)
        - Civilian MER Load Errors (v22: Error/Batch Employee Messages)
- Generate DCPS T&A Reports to verify acceptance of time by DCPS:
    - Invalid Transaction Report
    - Missing Time Report
- Generate DCPS Retro Reports:
    - Invalid Transaction Report
    - Conversion of Hours

4.5. SLDCADA Site Administrator Responsibilities

- Provide first line of defense for questions/problems.
- Maintain SLDCADA access.
- Restore access when users have moved shops.

- Unlock accounts.
- Maintain SLDCADA System News and Customer Service Message windows.
- Maintain Validation and Activity Profile settings.
- Assign Primary/Alternate Timekeepers and Alternate Supervisors.
- Coordinate with Yorktown operations for batch schedule changes.
- Inform SLDCADA users of software upgrades, system downtime, or changes to batch processing times.
- Only system administrators and a very few trusted users have full system privileges. Users who demonstrate both a need for full system privileges and an understanding of the responsibility that goes along with it might also have such privileges. Non-system administrators who share full system privileges with system administrators agree to guidelines such as notifying the system administrator of most changes made while using full system privileges.
- When notified by the user's chain of command, the system administrator will terminate employee access to SLDCADA immediately.

5. More information

For additional information, please visit the following Web sites:

- **Maintaining Effective Control Over Employee Time and Attendance Reporting (on GAO Web site):** http://www.gao.gov/new.items/d01186g.pdf
- **Freedom of Information Act:** http://www.defenselink.mil/pubs/foi/
- **PKI:** https://infosec.navy.mil/PKI www.defenselink.mil/nii/org/sio/ia/pki.html http://dodpki.c3pki.chamb.disa.mil
- **CAC:** www.dmdc.osd.mil/smartcard https://es.cac.navy.mil