

EPD Security Administrator Responsibilities

Security administration shall be carried out by the following agency positions:

1. Terminal Agency Coordinator (TAC) / Records Manager
 - a. Serves as point-of-contact for matters relating to CJIS information access; administers CJIS systems programs and oversees compliance with CJIS systems policies.
2. LEADS Rep / Records Supervisor
 - a. Conduct LEADS administrative duties for EPD and Communications.
3. Application Administrators
 - a. Understands integration points between various SunGard products and other integrated systems
 - b. Involved in decision making regarding system configuration to ensure operation of the system meets section and department business needs.
 - c. Responsible for ensuring resources are in place to train and onboard new users.
 - d. Assists with front-line application related support requests prior to their escalation to vendor support.
 - e. Determines application level access rights and controls configuration of user access rights.
 - f. Resets user passwords or performs other application related setup and troubleshooting tasks.
 - g. Serves as the primary liaison to SunGard support for their assigned product.
 - CAD – Designated Communications Supervisor
 - Enters Employee information into Employee Module
 - Enters CAD users into CAD module
 - MDC – Designated Patrol Supervisor
 - RMS – Designated Records Supervisor
 - Enters RMS users into RMS module
 - Completes process by attaching to employee record.
4. Authorized Requestors for network activation and password reset
 - Records Manager
 - Communications Manager
 - Technical Services Division Manager
 - Records Supervisor
 - Communications Supervisors
5. Authorized Requestors for network suspension
 - Records Manager
 - Communications Manager
6. Authorized requestors for prox card issuance/revocation can be located on the Facilities website.

7. Any requests related to personnel accessing public safety data (i.e, adding, deleting, change of permissions, employee separation) must be sent to the *Eugene Police Security Administration email group. Sensitive security requests may be made directly to the TAC.
8. The Technical Services Manager must notify ISD as soon as possible of any changes to designated security administrators.

*Note: HR must be copied on any sensitive requests.

Adding a New User

Appropriate background investigations, including a check of LEDS and NCIC fugitive warrant files, the Oregon computerized criminal history (CCH) system, and the AIRS system, must be conducted on all users requesting access to CJJ.

Background investigations shall be completed by the TAC or designees in accordance with POM 201.7. Disqualification factors include:

- Conviction of a Felony
- Conviction of a Class A Misdemeanor within the last 24 months
- If the individual is currently a defendant in a criminal proceeding involving a Felony or Class A Misdemeanor

New users must sign a confidentiality form, acknowledging the following:

- Passwords are confidential. If they are divulged, they need to be changed.
- Users are responsible for anything done with their user ID. Therefore it is critical that users utilize appropriate security to inhibit another user "hi-jacking" their system (i.e. utilizing session lock when leaving workstations.)
- System access and information is for law enforcement purposes only. Any use of the system for personal reasons will be subject to possible criminal prosecution, disciplinary action or dismissal.
- All transactions are logged and saved.
- Users must notify the Security Group when there are any indications that a security violation has occurred, lost password, etc.

The completed Confidentiality Agreement form should be scanned in the "user agreement" folder in Laserfiche.

Send requests for new user IDs to ISD via *Eugene Service Desk with the following information contained in the request:

1. Employee full name (including middle initial)
2. Employee ID Number
3. Start date
4. Department / Division
5. Full or Part Time
6. AFSCME or Exempt
7. Permissions / Sever Access (if known)

New user ID's will be formatted as CEPDXXX for Police and CEEYXXX for Comm Center.

Sealed passwords will be forwarded by the originating requestor.

- Patrol passwords can be forwarded to training.
- All others shall be distributed to hiring supervisors.

User Account Changes or Moves

Changes or moves to a user account are subject to the same considerations as new user additions and must:

- Come from an authorized requestor.
- Be verified by the application administrator that permission levels are based on least privilege.
- Must be documented by TAC in the access log.

Terminating, Suspending or Reinstating Users

Requests to terminate/suspend/reinstate public safety system accounts must be done by personnel equal to or higher than the Captain level. Requests of this nature must be directed to the TAC who will notify the appropriate Application Administrators.

Requests of a sensitive nature shall be directed to the TAC. The appropriate HR personnel shall be cc'd as deemed appropriate.

User Password Reset

When a user forgets their network passwords, a security liaison must request a reset with the Help Desk. In the event the user is unable to answer the questions, a security liaison must request a reset with the Help Desk.

Security Authorizations

It is the TAC's responsibility to:

- Make sure all workstations accessing CJ are located in a secure area and the information on the screen cannot be seen by unauthorized people.
- Ensure technical policies are applied appropriately (i.e., session lock, advanced authentication, and encryption.)
- Maintain record of TID numbers assignment and decommission.
- Conduct annual audits of user accounts and maintain a log of active users
- Document application permission or security level changes

To request a CJIS systems access workstation, send a request to the *Eugene Police Security Administration email group.

- Verify the agency has the additional license for the applicable Sungard applications
- Multiple workstations may be requested in a single form.
- All requests and configurations will be logged and retained by the TAC

Assigning User Identifiers

User identifiers include: network user id's, system user id's, passwords, and RFID cards

Ensure that:

- User logins are unique. No shared logins are allowed on public safety systems.
- The user has passed the proper background checks and fingerprints are on file.
- Only authorized personnel are allowed to add new users.
- The user identifier is issued only to the intended party.
- Authorized personnel receive and distribute user identifiers to the correct person.
- The user identifier is disabled automatically after a specified period of inactivity.
- User identifiers are archived for a minimum of one year.
- Lost or compromised user identifiers are to be immediately reported to the *Eugene Police Security Administration group.
- Default authenticators (if any) are changed upon system installation.
- Authenticators are changed periodically.

Approval date: _____

Last revision date: October 1, 2013

Next review date: _____

User Agreement

I, _____ hereby agree to abide by the State of Oregon laws,

(PRINT applicant name: first, MIDDLE and last)

Computerized Criminal History regulations and organizational and department policies regarding the confidentiality and dissemination of information stored in the Eugene Police Public Safety systems.

I agree that I will use the data that I have access to through the system only in the performance of my assigned job duties and I will not allow any unauthorized access to the data. I understand that to use it in any other way may be a violation of Oregon Revised Statute 244.040, which prohibits use of government office for personal gain or ORS 162.405-162.425, which prohibits abuse of public office.

I agree I will not release or divulge my personal security password to any person, agency or organization unless required by a direct order from my supervisor. If I release my security password by order of my supervisor, I will notify the agency TAC.

I understand if I knowingly fail to adhere to the above requirements, my personal security password will be suspended.

I understand that disciplinary and/or criminal action may be taken against me if I violate the confidentiality requirements set forth in this agreement. I understand that the agency maintains a complete record of all inquiries and updates I make to the public safety system for the purpose of enforcing confidentiality.

I agree I will notify my supervisor and the agency TAC if I am charged with a felony or Class A misdemeanor. I understand that if I fail to do so, my access to the public safety system will be terminated immediately.

SIGNATURE: _____ DATE: _____

Applicant

TITLE: _____ SUPERVISOR _____

LEDS CERTIFIED: ___ YES ___ NO

BACKGROUND INVESTIGATOR: _____ COMPLETION DATE: _____

SIGNATURE: _____ DATE: _____

TAC/Designee

Application CAD ___ RMS ___ MCT ___

Copy permissions of _____ (verify least privilege.)

