



# POLICY STATEMENT

Policy Statement 2003

Policy Area: Information Technology

Effective Date:

Approved: *Paul A. Quander, Jr.*  
Paul A. Quander, Jr., Director

*Susan W. Shaffer*  
Susan W. Shaffer, PSA Director

## ACCOUNT MANAGEMENT POLICY

### I. COVERAGE

This policy covers all permanent, temporary, and part-time employees of the Court Services and Offender Supervision Agency (CSOSA) and the Pretrial Services Agency (PSA) (hereinafter referred to collectively as the Agency), as well as interns, and contractors, and other non-Agency personnel who access the Agency automated information systems (i.e., email, servers, etc.). The term "employee" as used in this policy covers all of these categories. Employees with specific responsibilities under this Policy Statement include anyone accessing a computer through the Agency network (account users), application, server and network administrators, the CSOSA Information Security Officer, and account sponsors.

### II. BACKGROUND

This Policy Statement establishes the process for granting access to the Agency automated information systems. The CSOSA Office of Information Technology is responsible for administering, managing and monitoring automated systems accounts. The management and administration of automated system accounts is required by OMB Circular A-130.

### III. POLICY

Automated information system accounts will **only** be created and maintained for an employee if the employee requires such access to perform official duties. Access to all Agency automated information systems shall be controlled by the procedure described in this Policy Statement. Individuals not employed by the Agency or by an Agency support contractor shall be sponsored by a member of the Agency's staff with permanent civil service status prior to being approved for account access. The Request for Computer Access Form (Form CSOSA/IT-0001) must be used to create, change or delete an automated information system account.

### IV. AUTHORITIES, SUPERSEDURES, REFERENCES, AND ATTACHMENTS

#### A. Authorities

OMB Circular No. A-130 Appendix III (Security of Federal Automated Information Resources) [http://www.whitehouse.gov/omb/circulars/a130/a130appendix\\_iii.html](http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html)

B. Supersedures

None

C. Procedural References

Request for Computer Access (CSOSA/IT-0001)

<http://csosaweb/forms/computeraccess.pdf>

Password Reset Verification Form (CSOSA/IT-0003)

<http://csosaweb>

D. Attachments

Appendix A. General Procedures

**APPENDIX A  
GENERAL PROCEDURES**

A. Roles and Responsibilities

1. Account Holders

- a. The Agency automated information systems account holders are responsible for using accounts for performance of their official duties.
- b. Account holders must choose difficult-to-guess passwords. Passwords must not be in the dictionary and must not be a reflection of the account holder's personal life. All passwords must contain at least eight characters and must contain a combination of letters, numbers and special characters. Where systems support it, this minimum length will be enforced automatically.
- c. Password sharing is not allowed.

2. Agency Application, Server, Network and Account Administrators

- a. Create accounts for internal CSOSA systems within two (2) working days after the approval has been received from the Information Technology Security Officer. Approval of accounts for Sentry, WALES/CIC, NCIC, JUSTIS, and other external systems are subject to approval policies of the agencies responsible for those systems.
- b. Disable and delete accounts immediately upon the notification from the CSOSA Information Technology Security Officer.
- c. Ensure that password length and password reset policies are enforced.
- d. Use only System Administrator or privileged accounts when performing duties that require access levels higher than a normal user account (i.e., System Administrator accounts should be used for account creation, server and network software installations, etc.).

3. Agency Information Security Officer

- a. Review and approve Computer Access Request forms within one (1) working day. Forms that are incomplete will be returned.
- b. Monitor CSOSA IT staff for compliance with this policy.
- c. Initiate Help Desk tickets for the creation, disabling and deletion of accounts.

- d. The Information Technology Security Officer or IT Help Desk will provide the user the accounts and passwords.

#### 4. Agency Account Sponsors

Submit completed Request for Computer Access forms for new accounts, and employee terminations, transfers, resignations and retirements.

### B. General User Accounts

#### 1. Required Forms

- a. The Request for Computer Access form is used to create, change or delete automated information system accounts. The form can be located on the CSOSA Intranet at <http://csosaweb/forms/computeraccess.pdf> . The completed form must be submitted to Information Technology Security, 633 Indiana Avenue, N.W., 7th floor. Accounts shall be created after all signatures and approvals have been completed on the Request for Computer Access Form.
- b. New CSOSA account holders must submit a Password Verification Form (Form CSOSA/IT-0003 to authorize password resets. The form can be located on the CSOSA Intranet at <http://csosaweb> .

#### 2. Passwords

- a. Accounts will be set up to request a password change at the initial login (passwords must contain at least eight characters and must include a combination of letters, numbers and special characters). If the system does not require an automatic password change, the user is responsible for changing the password.
- b. Accounts will be set up to force a password change every 45 to 90 days depending on the system sensitivity level. If the system does not require an automatic password change, the user is responsible for changing the password, account holders will be notified periodically to change their password for these systems.
- c. Account holders will be notified of the account information and provided appropriate passwords. Account and password information will not be disseminated via e-mail.

#### 3. Account Review

Accounts for all non-Agency users (contractors and other Government or non-Government personnel) shall be reviewed by the Information Technology Security Officer every 90 days.

4. Disabling and Deletion of Accounts

- a. The Agency Account Sponsors will notify the Information Technology Security Officer upon the termination, transfer, resignation or retirement of an employee. This notification will be done by submitting the Request for Computer Access form.
- b. The Information Technology Security Officer will initiate a Help Desk Ticket and have it assigned to the appropriate Agency IT Department. The Help Desk Ticket will be closed once the account has been disabled or deleted.
- c. Accounts shall be disabled immediately upon the departure of an account holder or when an account holder's duties change and access is no longer authorized.
- d. Disabled accounts shall be terminated within five (5) working days.
- e. Accounts for Agency contractors shall terminate on the expiration date of their contract.