Security Liaison and Security Access Procedures

System Overview

The Security Access procedure provides instructions for Client Security Officers to obtain authorization for their personnel to access the NFC's computer facilities.

The NFC's computer access control system is designed to provide protection for NFC's computer resources by (1) identifying users who have authorized access, (2) controlling the use of system facilities, (3) protecting and insuring the integrity of system applications, and (4) restricting the use of these. NFC will grant authority to access the computer facility to individual users at the request of their organization (transmitted through the client's Security Officer).

Security Policy

USDA ADP Security Policy DR 3140 and the related ADP Security Manual DM 3140 require that managers of computer processing operations provide controlled access to the facilities and resources of the computer.

Users of a computing facility are to designate an ADP Security Officer (Client Security Officer) and an alternate ADP Security Officer that are responsible for the management of access to the computer.

Responsibilities

Clients will appoint a Client Security Officer that coordinates all requests for NFC computer access authorization.

Client Security Officer will:

- Obtain organization and/or owner authorization approval(s) to establish user ID according to the client's ADP security policy.
- Submit the request for computer access to the NFC Security Office through email at nfc.securityofc@nfc.usda.gov and send a copy of all security requests that affect CLER users to nfc.cler@usda.gov .
- Immediately notify NFC Security Office and CLER of any changes in the authority or of the termination of an employee in their organization.
- Consult with NFC's ISSO on security matters related to the use of the NFC's facilities.

NFC's Security Officer will:

- Grant authority to use/access the computer facilities based on the client's requirements.
- Establish, control, and maintain user identification.
- Log all unauthorized access attempts and furnish reports to the respective Client Security Officer for appropriate action.
- Monitor security concerns of the Client Security Officer related to the NFC's facilities and resources.

Access Administration

NFC will grant authority to use (access) its facilities to individual users at the request of their Client Security Officer. Every user will be assigned a unique identification which defines the specific information a user has access to based on job responsibilities, need to know, and the client's ADP security policy. Where appropriate, users are organized into functional groups based on their common access characteristics. The Client Security Officer is responsible for notifying NFC of any changes in their user groups. NFC logs any unauthorized access attempts and reports them to the Client Security Officer. If required, cancellations or suspensions of user identification should be handled immediately by telephoning the NFC ISSO. Communications relating to adds, deletes, or changes to user groups must go through the Client Security Officer to NFC. The NFC OSC Security may be reached by telephone at **1-800-767-9641, by fax at 1-888-245-4060,** or through E-Mail at nfc.securityofc@nfc.usda.gov.

Access to Facilities

The NFC facilities are batch job processing (BATCH), time-sharing options (TSO), integrated database management system (IDMS), and customer information control system (CICS) for automated transmission processing. Client personnel requiring access to NFC's computer facilities must identify their needs to the Client Security Officer.

All client personnel accessing NFC facilities are given an individual user identification ACcessor ID (user ACID), which must be password protected. Each user is responsible for managing his/her own password when it expires (every 60 days) which he/she must

change upon expiration or if the password is at risk. **Note:** ACcessor ID (user ACID) identifies both the user and the resources that the user is permitted to access.

Access to Resources

To access a given resource, a user **must** have permission to use the application. Access to an application includes access to files, databases, datasets, programs, terminals, nodes, etc. If access is being requested for an application that is owned by a client other than NFC, the requesting client **must first** obtain approval from the owner of the application.

Client Security Officer's Activities

The Client Security Officer submits requests for computer access, changes in authority, or termination of an employee, etc., to the NFC OSC Security Office. The NFC Security Office implements the requests and notifies the Client Security Officer when completed.

Establish User Access

The NFC Security establishes the access authority by interviewing the Client Security Officer. The communication with the Client Security Officer continues for administering additions and changes when necessary.

Telephone Inquiries

For questions about access authority, contact your Client Security Officer. When necessary, the Client Security Officer may contact the NFC OSC Security Office at **1-800-767-9641.**

Fax Inquiries

For questions about access authority, contact your Client Security Officer. When necessary, the Client Security Officer may contact the NFC OSC Security Office via fax at **1-888-245-4060**.

E-Mail Inquiries

For questions about access authority, contact your Client Security Officer. When necessary, the Client Security Officer may contact the NFC Security Office through E-Mail at nfc.securityofc@nfc.usda.gov.

Security Procedures

Users are assigned a unique user ID and password. The user ID/password combination identifies the user to CA Top Secret and allows him/her to access the resources required to perform the duties of the position. It is very important that the user ID/password be safeguarded. The following guidelines should be followed to secure user IDs.

Password Procedures

New Password. Must be at least six but not more than eight characters in length. It is recommended to use both alpha and numeric characters in the password and all characters should be entered lowercase.

Expired/Aging Password. CLER will display the message *PASSWORD EXPIRED*. It is highly recommended that the password be changed every 60 days.

Lost Password. If a user forgets his/her password, CLER will not allow him/her to access a facility. Users should not attempt to guess passwords. Client Security Officers should be notified to receive a new password. The Client Security Officer contacts the NFC Operations Security Center at **1-800-767-9641** to reset the User ID with a new temporary password.

Password Security. To protect the password:

- Users should memorize their user ID/password upon receipt.
- Users should destroy all written records of their passwords. Do not post passwords or maintain them in an unprotected dataset.
- Users do not share their user ID's or passwords with anyone. Personnel seeking the use of another's user ID/password combination should be directed to the appropriate security officer.
- Users should revise their passwords at regular intervals.

- Users are responsible for the use of the access authority contained on their user ID, therefore, they are responsible for the safeguarding of their user ID and password.

Reporting Problems. If violation messages are displayed:

- Do not clear the messages from the screen and do not press any keys on the keyboard.
- Copy all Top Secret Security (TSS) and message numbers and the accompanying text.
- Record all entries made prior to receiving the messages.
- Report the problem to the Client Security Officer.