

Security Access to Central Financial Systems Procedures

ESD's Security Officer(s)

1. The Security Officer (SO) shall be designated by the Superintendent/designee.
2. Any change or revocation of an existing Security Officer's system authority must be approved by the Superintendent/designee.

Requests for Standard Access

1. The SO reviews each management request for user access to ensure the request is consistent with the user's position and assigned job duties.
2. If the SO has a security concern, the SO notifies the user's manager and suspends processing until the concern is resolved.

Once the concern is resolved, the SO continues processing the request.

3. When requesting access, the employee's supervisor shall provide the following information for each user:
 - a. Full name of the individual;
 - b. The user's e-mail address and phone number;
 - c. The desired action: Add, Modify or Revoke;
 - d. The system(s) requested;
 - e. A brief explanation of the reason for each system requested.
4. If the request indicates the intent is to mirror another user's profile, the request must specify the exact access for the new user by completing the information 3 a.-e. for each system requested.
5. The SO will deny access if any required information is missing and return incomplete information to the requesting party.
6. All requests will be kept on file.

Requests to Change or Reset Passwords

Users may change passwords or request a password reset from the SO.

Security Reviews

1. Security reviews shall occur annually in July and when there is a change in Security Officers. The ESD Security Officer verifies the correctness of the access granted to the users and checks with the users' managers to determine if the level of access is still appropriate. The reports shall be forwarded to the SO's supervisor.
2. The ESD Security Officer shall report and record any security changes.
3. The ESD shall retain copies of the reports for reference purposes.