Security Awareness Message
USER ACCOUNT MANAGEMENT
April 2012

User account provisioning is a business process for creating and managing access to resources in an information technology (IT) system.

OCFS and its partners engage in workflow-based account provisioning – where the designated person gathers the required approvals from approvers/ supervisors before granting a user access to an application or data. These generally include Lan Administrators and Security Coordinators.

Automated account provisioning – OCFS uses Webstar (Web Enhanced Basic Security to Authorize Resources) for the CONNECTIONS application to register users through its interface.

User account management- Every district and agency should identify a uniform process for user account management, including provisioning, de-provisioning and exceptions;

Provisioning: When a worker comes on board

- The LAN administrator usually puts the worker into Webstar into a CONNECTIONS organizational unit.
- An overnight batch process occurs and the worker is put into an N01 unit in CONNECTIONS-The worker has no security or access at this point.
- The Security Coordinator assesses the worker's needs for access within CONNECTIONS based on job responsibilities. There are tools to assist with this assessment (Security Outreach and Review (SOaR) **New Employee Security/ Access Survey)**
- The worker should be given the least amount of access they need in order to complete their work.
- The worker should also be informed that they are to access only what they have an authorized purpose to access.

Change Management

- If a worker's responsibilities change and they no longer need certain access, it should be removed- For example if a protective worker becomes a preventive worker, their cps business function profile should be removed in a timely way.

De-provisioning

- When a worker leaves the agency or no longer needs access to CONNECTIONS they should be end dated or their User ID disabled in CONNECTIONS right away. This prevents a worker from accessing information that they no longer have an authorized need to know. With remote and web access to CONNECTIONS this timely function becomes critical. NOTE: If the worker is disabled through Webstar they will no longer have access to CONNECTIONS even if they have not been end dated.
- Keep in mind that you may have to reassign a worker's cases and get rid of to-dos in order to end date staff but it is necessary to do this right away.
- If a worker is on leave, their ID should be disabled and re-instated only when they return. If another worker needs to do the work in their absence there are ways to provide access for example through Unit Hierarchy access.