Procedure: Account Management for Terminated and Transferred Employees

Purpose:

The UF Account Management Standard requires that accounts and authorizations be promptly modified when a user's job duties or employment ends. Many users retain affiliations upon termination of employment which prevent their Gatorlink account from being disabled (i.e. Alumni). Processes are in place to automatically remove assignable enterprise roles from the accounts of former employees.

These procedures address removal of unit assigned enterprise roles, and permissions and authorizations controlled by unit-level mechanisms.

Procedures:

Departmental Security Administrators (DSA):

A Security Role Verification Report is sent to the DSA of departments to which an employee transfers from within the university. The DSA is responsible for reviewing and updating enterprise security roles for transferred employees. Enterprise security roles that are no longer needed for the new position should be removed within three business days of the employee's start date in the new department.

Unit IT:

Locally granted permissions and authorizations that are no longer necessary are expected to be removed within 24 hours of an employee's employment end-date. This includes permissions and group assignments within Active Directory, as well as any other systems or software controlled by the unit, including cloud services. Access to departmentally controlled resources must be terminated regardless of whether the access was granted to a Gatorlink or other account. If the terminated employee had access to accounts with shared passwords, the UF Account Management standard requires that the password for those accounts be changed to prevent use by the terminated employee.

For timely notice of transferred and terminated employees, department IT staff can subscribe to receive an enterprise report for the specific Department IDs they are responsible for. Refer to the *Running and Scheduling the Department Terminations and*

Transfers Report document for instructions on how to configure and schedule the report for automated delivery. This report should be set for daily delivery and will include all employees that terminated or transferred within the past 14 days, for the selected Department IDs. Departments should assign staff to review this report daily and take appropriate action and include coverage for when the person with primary responsibility is out of the office.

References:

UF Account Management Standard

UF Admin Memo: Timely Deactivation of Access Privileges

Running and Scheduling the Department Terminations and Transfers Report