

Title: Termination and Account Inactivation Procedure

Frequency: Weekly

Procedure:

A. Inputs that drive termination and account inactivation processing:

1. HR Feeds. HR feeds are received by the information security group from various sources. Among other things, HR feeds indicate the employment status (active / terminated) of personnel. During weekly termination processing, newly terminated employees from each HR source are identified.
2. Inquiries About Sponsored Users. Sponsored users are either recently hired employees who do not yet appear in HR feeds, or people who perform services for NewYork-Presbyterian Hospital and affiliated institutions, but who do not appear in any HR feed that the Information Security (IS) group receives. Cornell and Columbia students are also considered sponsored users. Sponsors must renew sponsorship of sponsored users at least every 6 months (default is 4 months). The IS group keeps track of sponsored accounts in our central user database, and sends email to sponsors approximately 2 weeks prior to the expiration date of any of their sponsees to inquire if the sponsorship should be renewed (i.e., extended for up to 6 months) or if the sponsee's accounts should be inactivated. Sponsor responses are recorded in the user database, and acknowledged nonrenewals are collected as an input source for termination processing. If a sponsor does not respond after two notices (the second notice is sent approximately 1 week prior to the expiration date) it is considered a nonrenewal.
3. System-account Lists. In addition to HR feeds, the IS group receives/retrieves user account lists from various systems. These account lists are processed weekly and accounts of persons who are listed as terminated in all HR sources and who are not sponsored users (see item 2 above) are flagged for inactivation.
4. Audit Logs. Audit logs from various applications are automatically retrieved and processed daily. One component of this processing involves checking if any login ids appearing in the logs are owned by persons

listed as inactive in our user database. If any such ids are identified, the account information is prominently listed in an audit-alert email sent automatically to IS personell, who respond as soon as possible.

5. Account-Inactivity Reports. The IS group follows the policy that accounts that have not been used for 3 months (93 days), and accounts that were created but never used for 21 days or more should be inactivated. Certain system-account lists (see item 3 above) include information about account creation date and date of last login. Such lists are used to create account-inactivity reports, which are in turn used to drive account inactivation.
6. Adhoc call-ins or emails. A small number of inactivations result from directors / managers / sponsors notifying the helpdesk and/or IS personell of terminations. These inactivations are recorded in the central user database when received, and also serve as an input for weekly termination processing.

B. Generation and distribution of weekly termination report:

Each week, the above input sources are aggregated and used to create a termination report. This report lists recent terminations sorted first by HR source, then by business unit within the HR source (applicable for NYP HR), and then by name. Title, department, and the user's center-wide login ID (CWID) are also listed. If the user is active in some other HR source, that is noted.

A section of the report also includes information about sponsored-account nonrenewals (item A.2 above) and adhoc call-in/email terminations (A.6).

The report is distributed via email to system and application owners and managers, who are responsible to inactivate the accounts.

C. Automated account inactivation of certain systems:

Certain systems have automatic or semi-automatic account inactivation components in place that are triggered by weekly termination processing. These include:

1. NYP LDAP (e.g., WebCIS, West campus Amicas)
2. OAC LDAP (e.g., nyp.org Email, East campus Amicas)
3. Siemens mainframe (e.g., Eagle)
4. Lawson Materials Management

D. Distribution of accounts-to-inactivate lists to targeted groups:

System accounts that are recorded in the central user database, and the system-account lists mentioned in Item A.3 above, are used to create accounts-to-inactivate lists for specific systems. These lists are distributed to the appropriate managers of those systems, who are responsible to inactivate the physical accounts.