Atypical Employee Termination
Process and Information Requested

When an individual's employment is terminated without the normal transition period, steps need to be taken to ensure that the employee's access to institutional data and resources is restricted concurrent with the termination. Prompt removal of the any access privileges protects both the school as well as the former employee from any allegation(s) of misuse of institutional resources.

To facilitate the efficient removal of access, Computing Communications and Information Technology (CCIT) requests that the individual coordinating the termination provide the attached information at least 24 hours before the employee will be notified of their dismissal. This information can be provided to Phil Romig in his role as the Chief Information Security Officer (CISO) or Ed Zucker in his role as the coordinator of CCIT's Identity Management team. CCIT leadership will use this information to ensure that the required engineers are available at the appropriate time. CCIT engineers are told that an employee termination will occur on the given day/time but will not be told the identity of the employee until after the dismissal meeting with the employee is scheduled to begin.

Once the dismissal meeting has begun CCIT will take the following steps:

1. Leadership will let those involved in the process know the name and home department of the employee.
2. Someone from CCIT (typically someone from the Identity Management (IDM) team) will create a Helpdesk support ticket containing the attached information. The customer on the ticket will be employee's supervisor.
3. The Identity Management team will randomize the employee's "MultiPass" credentials and prevent use of the Password Recovery feature. This prevents the employee from logging into:
   a. Computers that are members of the ADIT domain.
   b. The Exchange email system used by employees.
   c. Trailhead and the associated Self-Service Banner portal (SSB). Note that this limits the employee's ability to access existing payroll and tax information.
   d. Resources that use the federated authentication services. Some of the more prominent services in this category include Canvas, Microsoft 365, <others>
   e. Centrally managed Linux systems.
4. The Enterprise Systems team will remove all access privileges for Banner and related systems.
5. The Network team will remove all devices registered to the employee, preventing network access not available to the general public.
6. The telecommunications team will reset the employee's voicemail PIN and call the supervisor with the new PIN.
7. If desired the email administrator will:
   a. Arrange for an "Out of Office Message" notifying senders of the employee's absence.
   b. Arrange to have new messages forwarded to the employee's supervisor.
   c. Provide access to the employee's existing messages to the employee's supervisor.
8. If desired, the Windows team will provide access to the employee's home directory to the employee's supervisor.

In addition to the above steps it is critical that the former employee not be allowed unsupervised access to their computer, laptop and/or tablet after the dismissal meeting. Removing access as described above will not protect these devices. CCIT recommends shutting down these devices during the dismissal meeting. If that is not possible, the employee should be supervised when around their systems and the systems should be removed from the network as soon as possible.

Most employees keep some personal information on their work computer (pictures, email sent to their work address by mistake). If the employee requests access to this type of information the supervisor should ask CCIT for help in providing the requested information. This should be done via an update to the helpdesk ticket created in step 2.

It is important to understand that the process described removes the employee from the CCIT's normal termination process. As a result, the employee's accounts will not be removed as they typically would and the accounts will remain in limbo until the supervisor asks that they be removed. CCIT requests that this delay not be too long. Files and other information belonging to the employee should be transferred into the new owner's direct control. The supervisor should notify CCIT that they are ready to have the accounts purged by updating the ticket created in step 2 as soon as possible.

Atypical Employee Termination
Process and Information Requested

To prepare for an atypical termination please call Phil Romig at (303) 273-3866 or Ed Zucker at (303)384-2460 least 24 hours before the termination meeting will take place. At a minimum we will ask for the following information:

(1) Employee’s name:

(2) Employee’s username:

(3) Home Department:

(4) Day and time of the dismissal meeting:

(5) Supervisor’s Name:

(6) Supervisor’s username:

(7) Does the employee have access to Internet Native Banner (INB)?

(8) Are there other systems the employee has access to that might use unique credentials?

(9) What should be done with new email sent to the employee’s address:

a. Forward to the Mines email address: _______________________________

b. Rejected and returned to the sender.

c. No change (it will be delivered to the employee’s inbox).

(10) Should an out-of-office message be sent in response to new email sent to the employee. If so, what should the message be:

(11) Should the supervisor be given access to the employee’s existing messages (the employee’s mailbox will appear as a new mailbox inside the supervisor’s email client).

(12) Should the supervisor be given access to the employee’s home directory?

(13) Should the telecommunications department provide the employee’s voicemail PIN to the supervisor?

(14) Should the telecommunications department forward the employee’s calls to a different extension? If so, which one?

(15) Do you expect that the terminated employee will need access to any computing resources after the termination meeting? If yes, which systems?

(16) Is the employee an instructor (if so the Instructional and Learning Technologies team will need to work with the replacement instructor(s) to transfer control of any educational resources).

Document created 19-June-2018

Questions or comments should be directed to security@mines.edu