| | | |
|---|---|---|
| COLORADO SCHOOL OF MINES | **Computing Account Termination Procedures** | |
| | **Responsible Administrative Unit:**<br>Information & Technology Solutions | **Contact:**<br>Monique Sendze CIO, ITS<br>msendze@mines.edu |

## 1.0 PROCEDURE PURPOSE

The Colorado School of Mines ("Mines") is committed to the protection of Mines information assets and Mines information resources from unauthorized access or damage. As part of this commitment, Mines has established the following procedures regarding the removal of access to computing resources.

## 2.0 PROCEDURES

The following procedures cover the removal of user access for normal terminations, which are voluntary in nature. De-provisioning can vary based on role and type of user account.

**2.1 Staff/Faculty/Third Party Terminations.** Upon notice of termination, an individual's department head or manager should work with the departing employee/contractor to arrange for the preservation of all business-related files from the employee's/contractor's network space and email inbox.

- Upon learning of a staff/faculty/third party's intended termination of employment/contract, the department manager must immediately submit a Separation Notice to Human Resources (HR). Use of the HR Separation Notice will allow the Mines administrators that are responsible for access controls (e.g., ITS, MAPS, etc.) to disable the staff/faculty/third party's access to the applicable Mines resources. Providing the HR Separation Notice timely may help prevent unauthorized access, effective within 24 hours of the Termination Date in Banner.
- The staff/faculty/third party will have until their last day of employment/ contract to remove their personal information or email from Mines computers or servers.
- Departing employees/contractors must not remove or delete any data that is:
  - not their own
  - necessary for the operation of the department or college
  - required by Mines retention policies
  - protected by federal or state law, or
  - placed under a Preservation of Evidence Directive (PED)

- The department head or supervisor may request access to the staff/faculty/third party's computer, electronic data storage locations, or email account for business continuity purposes from ITS **within 30 days of the employee's/contractor's departure.** This includes any requests to transfer/migrate email or other processes from the departing employee/contractor to a different individual in the department. **ITS will not provide such access automatically**.
- The manager or department may copy, store, or delete any data that is not required to be kept by applicable policies or laws. If a PED applies to any staff/faculty/third party's data or email, the contents of the applicable folders may not be altered until the PED is lifted.

**2.2 Part-time Faculty Inactive Teaching Status.** If a faculty member is not teaching consecutive semesters (Fall/Spring, excluding the Summer) at Mines, ITS will deem their account status as "Inactive." Their account will be allowed to remain active for one (1) semester following the last day of the last semester they taught at Mines. They will have full access to their Mines Account and to their Mines email account. If the faculty member does not teach at Mines following that one (1) semester hiatus, **the academic department** must terminate their account in accordance with the procedure described above for Staff/Faculty/Third Party Terminations.

**2.3 Full-time Faculty Leaves.** Any faculty member who is on approved leave will have full access to their Mines Account and email. At the end of their approved leave time, the account will follow the procedures described above.

**2.4 Account Transfers.** Staff changing departments are not subject to these account removal procedures. However, to avoid unintended removals and optimal transition of access, ITS must be notified immediately using the ITS Account Change Form and corresponding Service Description for further details.

**2.5 Suspension of Account or Access.** ITS reserves the right to temporarily disable or suspend any account that may pose a security risk to Mines' network or data, in its sole discretion. If the risk cannot be reasonably mitigated, ITS reserves the right to permanently delete any account that may pose a risk to Mines' network or data.

## 3.0 HISTORY AND REVIEW CYCLE

The procedures within this document will be reviewed at least annually or as needed by the Responsible Administrative Unit.
Issued: January 31, 2020.