ACCESS TO TECHNOLOGY ASSETS

Purpose

The purpose of this procedure is to define processes for granting access to and safeguarding the District's electronic assets. These technology resource assets include software as well as confidential and sensitive data contained on District and vendor networks and computers related to students, faculty and staff in addition to research and other intellectual property.

It is the practice of the District to provide necessary access to technology resources that are required for the performance of job duties. To facilitate access, the District Information Technology Department maintains a central account authentication system that is used at all sites for employees to identify themselves to network and other centrally managed software systems such as Colleague, email and learning management systems. Control of authorization within each of the Districtwide systems is provided on an as-needed basis upon approval from appropriate manager(s).

Maintaining accurate, effective access controls is critical to protecting District technology resources. Ongoing communications between managers, college/District Human Resources and the Information Technology departments is essential in maintaining viable controls.

This procedure is intended to align District processes with risk mitigation best practices as well as ensure District compliance with governmental and contractual regulations including, but not limited to:

- Family Educational Rights and Privacy Act (FERPA);
- Gramm-Leach-Bliley Act;
- Health Insurance Portability and Accountability Act (HIPAA);
- California SB 1386 – California Database Breach Act; and
- Payment Card Industry Data Security Standards (PCI-DSS).

Scope

A. This procedure is applicable to all personnel employed in any capacity by the District and to all software and electronic assets owned/rented by the District.

B. For procedures related to access control devices, refer to Business Procedure 10.53. For procedures related to non-technology related assets, refer to Business Procedure 10.55. For Employee Check-In, Employee Exit, and Asset and Access Device Assignment forms, refer to Business Procedure 10.56. These procedures are all related, and all should be reviewed when a new employee is hired by any CCCCD Unit. When changes are made to this procedure, all related procedures should be reviewed to ensure they remain consistent.

Access

Access to electronic assets will be granted at the minimum level required which allows for the routine performance of assigned job duties. Exceptions may be granted for cause and must be documented and authorized.

Recordkeeping

Maintaining accurate records of the access granted is critical to protecting District electronic assets. The District Information Technology Department will maintain records for tracking access granted, revised and revoked for Districtwide resources. Each college information technology unit, in conjunction with division managers, will be responsible for tracking and maintaining records on access to local technology assets.

Definitions

The following definitions are used in this procedure.

A. Technology: Technology refers to all technology resource assets, which include all software and any confidential or sensitive data contained on District or vendor networks and computing devices related to students or employees. This includes information related to research and other intellectual property.

B. College HRA: Human Resource assistant(s) at a college.

C. Staff Assistant: Human Resource staff assistant(s) at the District Office.

D. Returning Employee: Any employee who has had their account access revoked or deleted due to inactivity and whose manager has requested reactivation.

E. Districtwide Technology: Any technology for which the District Information Technology Department is responsible, or technology asset located in the District Information Technology Department.

F. Local technology: Technology that is located and controlled at the campus, such as shared drives, projectors, presentation stations, printers etc.

Granting Access to Districtwide Technology

The following processes define how access to technology shall be granted to employees Districtwide.

A. New permanent employees – classified professionals, faculty, and managers
   1. College HRA/staff assistant enters basic information about new employee into Colleague.
   2. Information entered in Colleague will trigger:
      a. email/portal account creation.
      b. auto-generated email to employee’s manager requesting that they complete an ‘*account request*’ form; and
      c. confirmation email sent to employee’s manager from District Information Technology once account setup is completed.

B. New temporary employees - classified hourly employees, student workers, gratuitous employees, or employees from a contract agency
   1. Manager sends a “request to process” to college HRA/staff assistant
   2. College HRA/staff assistant enters basic information about new employee into Colleague
   3. Information entered in Colleague will trigger:
      a. email/portal account creation.
      b. auto-generated email to employee’s manager requesting that they complete an ‘*account request*’ form; and
      c. confirmation email sent to employee’s manager from District Information Technology once account setup is completed.
   4. College HRA/staff assistant sends a “requisition” to District Human Resources with a specified END DATE, if earlier than June 30 of the current fiscal year.
      a. District Human Resources will enter June 30 of the current fiscal year as the END DATE on the wage line, unless an earlier END DATE is provided.
   5. Student workers and gratuitous employees shall not be granted access to confidential data, including the Colleague system.

Revoking Access to Districtwide Technology

The following processes define how access to technology shall be revoked for Districtwide technology systems:

A. Account Inactivity and Deletion

1. Any employee account, regardless of employee classification, that has not been used (logged into) for 90 days shall be deactivated. Employees and their managers will receive a warning before accounts are deactivated. To reactivate an inactive account, the employee's manager should send a request to District IT.
2. Accounts that are inactive for 12 months shall be deleted.
3. Exceptions pertaining to the account deletion or deactivation protocols may be made in extenuating circumstances or when it is in the best interest of the District.

B. Permanent Employee Resignation, Termination or Retirement

1. Accounts will be deactivated the day after the employee's last day of work as specified in the resignation or termination letter.
2. 30 days from employee's resignation or termination date the account shall be deleted.
3. Employees who retire from District will continue to have access to email but access to other systems/software will be removed the day after their last day of work.

C. Part-Time Faculty (Instructional)

1. During November of each year, District Information Technology will deactivate email/portal accounts for part-time faculty who are not assigned to teach a section in current or future terms.
2. To reactivate an inactive account, the employee's manager should send a request to District IT.
3. Any telephone voicemail box will be deleted. A new voicemail will be assigned upon return.

D. Hourly Classified, Part-Time Non-Instructional Faculty, Student Workers, and Gratuitous Employees

1. During July of each year, District Information Technology will deactivate email/portal accounts for all part-time, non-instructional employees which an expired wage line in Colleague.

Granting Access to Local Technology

College information technology, in conjunction with managers, will be responsible for providing access to local technology assets and maintaining appropriate records.

Deactivation of Access to Local Technology

College information technology staff will deactivate access to local technology for individuals that have been deactivated from access to Districtwide technology, as described above.

Periodic Audit

These records are subject to periodic audit by Internal Audit Services.

Historical Annotation:
Adopted: 1/13/15
Revised: 11/12/24

Related Board Policies:
Board Policy 5036

Related Procedures:
Business Procedure 10.53, 10.55, 10.56