ROUTING
All Schools and Offices

TITLE: How to Obtain a District Single Sign-On and E-mail Account

NUMBER: REF-1438.3

ISSUER: Shahryar Khazei
Chief Information Officer
Information Technology Division

DATE: July 13, 2017

MAJOR CHANGES: This document updates version 2.0 dated February 2, 2011 to reflect new procedures and information.

PURPOSE: The purpose of this Reference Guide is to inform District personnel about the process and procedures for obtaining a District-provided Single Sign-On (SSO) and E-mail account. Following the Procedures statement, this Reference Guide is divided into sections to provide information for acquiring SSO accounts for different District roles, in the following order:

- SSO accounts for employees
- SSO accounts for students
- SSO accounts for parents
- SSO for non-District employees

Account administration follows the above sections for:

- SSO accounts for students
- SSO for non-District employees

PROCEDURES: The Information Technology Division (ITD) provides SSO accounts to all District employees, students of K-12 schools, parents of students, and Non-District Employees (contractors, charter employees and community volunteers) who are required to sign into the District lausd.net domain to conduct District-related business. All users receiving SSO accounts from ITD are required to comply with BUL-999.11, the District's "Responsible Use Policy for District Computer and Networking Systems" (RUP). Procedures for obtaining a SSO account are described for each group below.

EZ Access (http://ezaccess.lausd.net) is a centralized system designed to let non-District employees request SSO account and email account, and to let employees/non-employees request authorization to various District applications. It reduces and sometimes eliminates the need for paper forms.

The SSO Self-Service and Account Management (SSAM) website is used for password resets by users, and account managers, and is located at https://mylogin.lausd.net. Passwords for SSO/e-mail accounts are valid for 180 days after either the account is activated or after each password reset. An expired password will prevent users from accessing District applications. Password resets should not exceed 3 attempts in a 24 hour period in order to avoid issues with logging into Google Apps and Office 365.

SSO ACCOUNTS FOR EMPLOYEES

All active District employees automatically get an SSO account and an accompanying email account, which can be activated and managed by visiting the SSAM Console. Employees need to verify with their Human Resource (HR) representative that their assignment has started. Employees will answer questions to verify their identity and select a security image. The e-mail address will be the employee's SSO account name plus the domain (e.g. user.name@lausd.net). E-mail may be accessed using a web browser at https://mailbox.lausd.net. More information about ways to access e-mail can be found at http://achieve.lausd.net/Page/2127.

If the employee experiences difficulty using the SSAM Console, they may request assistance by contacting the ITD Customer Support Services Center (IT Help Desk) at http://helpdesk.lausd.net or (213) 241-5200. IT Help Desk personnel will ask for 1) employee number, 2) user account and 3) response to security questions.

District SSO accounts for employees are disabled after ITD receives an automated notification that the employee no longer works for the District or a request by an Administrator is received. If an account is disabled in error, the employee may request the account be re-enabled by contacting the IT Help Desk. For contact options, please go to http://achieve.lausd.net/Page/286.

It is recommended that employees log into their e-mail at least once a week to avoid missing a notification e-mail informing them of the upcoming password expiration date. The notification e-mail is sent daily starting 14 days from the expiration of the password. Failure to reset password prior to expiration, will impact ability to access District applications (i.e. MiSiS, LRP, Welligent, etc.).

SSO ACCOUNTS FOR STUDENTS

All active District students, have an account provisioned upon enrollment. Students may activate new SSO accounts by visiting the SSO Console at https://mylogin.lausd.net. Each student's e-mail account can be activated and managed by the student, and the principal may designate a school employee to manage students' accounts as the school's e-mail sub-administrator (see SSO ACCOUNT ADMINISTRATION FOR STUDENT ACCOUNTS).

Students will use their birthdate, student ID number and a unique 4-digit personal identification number (PIN) – distributed by the school – to activate and set up their account. Please note: a valid RUP must be on file at the school site in order to distribute a PIN to the student. Further details regarding this process as well as accessing student PINs is available for teachers and school administrators at http://tinyurl.com/ssoreset.

All student account passwords expire every 180 days. In order to avoid interruptions in instruction it is recommended that teachers and administrators remind students to change their passwords 2-3 weeks before the end of each semester (before winter break and end of school for elementary schools).

SSO ACCOUNTS FOR PARENTS

Parents of active LAUSD students can optionally sign up for a District SSO account in order to gain access to their children's academic information via the Parent Portal at https://passportapp.lausd.net/parentaccess/. Accounts can be activated by parents via the self-service portal at https://mylogin.lausd.net/. A personal email address is required to register for a District account. A guide for resetting a password as a parent can be obtained at http://achieve.lausd.net/Page/10470 (Resetting an LAUSD Account). The guide is available in both English and Spanish.

SSO ACCOUNT REQUEST FOR NON-DISTRICT EMPLOYEES

Contractors, charter school & non-public school (NPS) employees or non-public agency (NPA) providers, and authorized community volunteers, can request an SSO account to access District applications or systems, such as MiSiS and Welligent, and to log onto computer workstations in office locations, including the Beaudry building and Local District Offices. A District email account can also be requested along with the SSO account, if necessary.

A Non-District Employee SSO account and the optional email account can be requested on-line using EZ Access. An e-mail account with the domain from the Non-District employee's organization (i.e. @mycharter.org or @privateschool.org) is required for registration.

To obtain an SSO Account:

1. Go to https://ezaccess.lausd.net and click on "EZ Access for Non-LAUSD/Charter Employees"
2. Click on "I do not have Single Sign-On Account"
3. Complete the information in all required fields
4. An automated e-mail will be sent out to the SSO Site Administrator requesting approval with a CC to the e-mail address provided on the application form

5. A subsequent email will be sent with further instructions once the account has been approved and processed

To check the status of the request:

1. Return to the EZ Access page
2. Indicate whether or not you have been an LAUSD employee
3. Indicate whether or not you have an existing Single Sign-On account
4. Select "Check Status of EZ Access Request."
5. Complete the four (4) fields with the same information provided in your application.
6. Press "CHECK ACCOUNT"
7. The status of your current request will appear below

Non-District employee accounts are valid for either one (1) year from the date they are created or the expiration of the contract with the District, whichever comes first. The SSO system will send a notification of impending account expiration.

It is the responsibility of the SSO Site Administrator to immediately notify the IT Help Desk at http://helpdesk.lausd.net or call (213) 241-5200 if the account requires termination prior to the scheduled expiration date.

SSO ACCOUNT ADMINISTRATION

Principals can designate District employees to manage student accounts for their specific school as an e-mail administrator (see below). Department managers and administrators can apply to become approvers for Non-District Employees for their specific location (site administrator) via EZ Access (see below). Account administration is performed via the SSAM Console.

SSO ACCOUNT ADMINISTRATION FOR STUDENT ACCOUNTS

By default, the principal is designated as the school's e-mail sub-administrator. To change the designation to another school employee, follow the instructions below.

Designating a Student SSO Account Sub-administrator

1. The principal or administrator can download the School E-mail Sub-Administrator User ID Authorization Request form from https://ezaccess.lausd.net (if not already assigned as the approver).
2. The employee being designated as the sub-administrator completes the online form
3. The school principal endorses the request by approving the online form

When this request is processed, additional privileges will be added to the SSO account of the sub-administrator. The school sub-administrator can log into the SSAM Console to perform the following functions:

1. Reset forgotten passwords when the student is unable to use self-service
2. Reset locked accounts when the student is unable to use self-service
3. Disable accounts when parents do not allow the student Internet access in school, or for an administrative reason

SSO SITE ACCOUNT ADMINISTRATION FOR NON-DISTRICT EMPLOYEE

A registered Site Administrator and site location are required in order to process non-employee SSO requests. The role of Site Administrator requires a hard paper copy to be processed by ITD, with at least one (1) first level approver per site. LAUSD offices using contractors (non-employees) must designate a District employee as a Site Administrator for each branch office to approve or deny such requests. A Site Administrator may assign up to three (3) additional site approvers. No SSO account requests can be submitted for a District location until the process below is completed.

To begin, the identified Site Administrator will:

1. Go to the EZ Access site (https://ezaccess.lausd.net)
2. Download the EZ Access Quick Start Guide and the EZ Access Site Administrator request form
3. Follow the instructions on the form to complete the application

Once the applications have been processed, the Site Administrator will receive an email notification. The Site Administrator may then setup and verify the site information on the EZ Access website and begin managing SSO requests for the location. Site administrators should login at least once a day to view pending requests from requestors at their site. ITD Security will then review these requests. All requests processed by ITD each day will be available the next day for self-activation.

From the EZ Access site (https://ezaccess.lausd.net) SSO Site Administrators and Approvers can:

- Lookup SSO account requests
- Approve/deny SSO account application requests
- Manage site access
- Set up roles
- Lookup site information

COMPROMISED ACCOUNTS

When a District account is identified as compromised, action is taken by the technical team to lock down the account preventing or limiting the user's access to District resources (i.e. email, MiSiS, BTS). The affected user must open a service request with the ITD Helpdesk in order to regain access to their District account. The user will be required to reset their password and take a short Cyber Security training session prior

to account restoration.

RESOURCES: The following websites have additional detailed information:
http://achieve.lausd.net/Page/286
https://ezaccess.lausd.net
https://mylogin.lausd.net/

ASSISTANCE: For further information, please contact the IT Security Office at (213) 241-5200.