

How to Access the SF Employee Learning Portal

A Quick Guide for UCSF Faculty, Staff, and Trainees at ZSFG



Reminders

- Use Firefox, Microsoft Edge, or Chrome
- Turn Off Pop-Up Blockers



Step 1

Visit: <https://zsfg.ucsf.edu/sflearn>

UCSF University of California San Francisco

ZUCKERBERG SAN FRANCISCO GENERAL Hospital and Trauma Center

About ▾ Research ▾ UCSF Medical Education at ZSFG UCSF Pride Hall Resources ▾ Newsletter

News

Home > Resources > Annual Learning Training

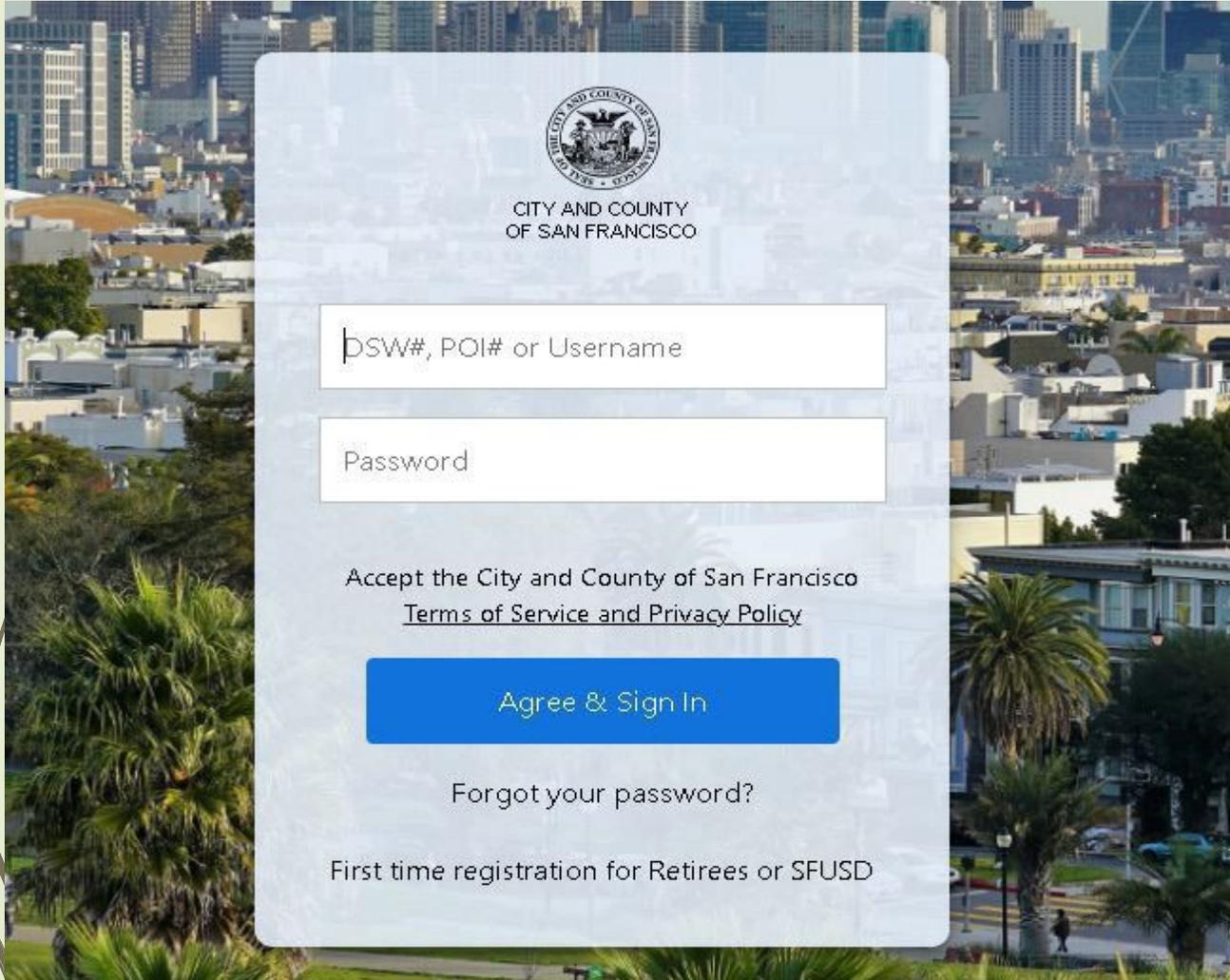
Annual Learning Modules and Compliance & Privacy Training

Annual Learning: Launching June 21, 2024 | Compliance & Privacy: Launching August 1, 2024

ANNUAL LEARNING LOGIN ← Select Link

CCSF Login Page

If you know your POI# and Password, skip to Step 6

A screenshot of the CCSF login page. The page features a light blue background with a faint cityscape. At the top center is the City and County of San Francisco seal, with the text "CITY AND COUNTY OF SAN FRANCISCO" below it. There are two input fields: the first is labeled "POI#, POI# or Username" and the second is labeled "Password". Below the fields is a link for "Terms of Service and Privacy Policy". A blue button labeled "Agree & Sign In" is positioned below the link. At the bottom, there is a link for "Forgot your password?" and a note: "First time registration for Retirees or SFUSD".

- Enter UCSF POI#
Contact: [Department Manager/ Champion](#) or [Trainee Administrator](#) for Assistance

- Enter Password

First Time User?

Contact DPH IT for temporary password, 628-206-7378

Previous User and Forgot Password?

Select 'Forgot your password?' link

- Select 'Agree & Sign In'

IF you entered both POI# and Password

Forgot your password? Page

Forgot your password?

Enter username for password reset.

DSW or POI# or USERNAME

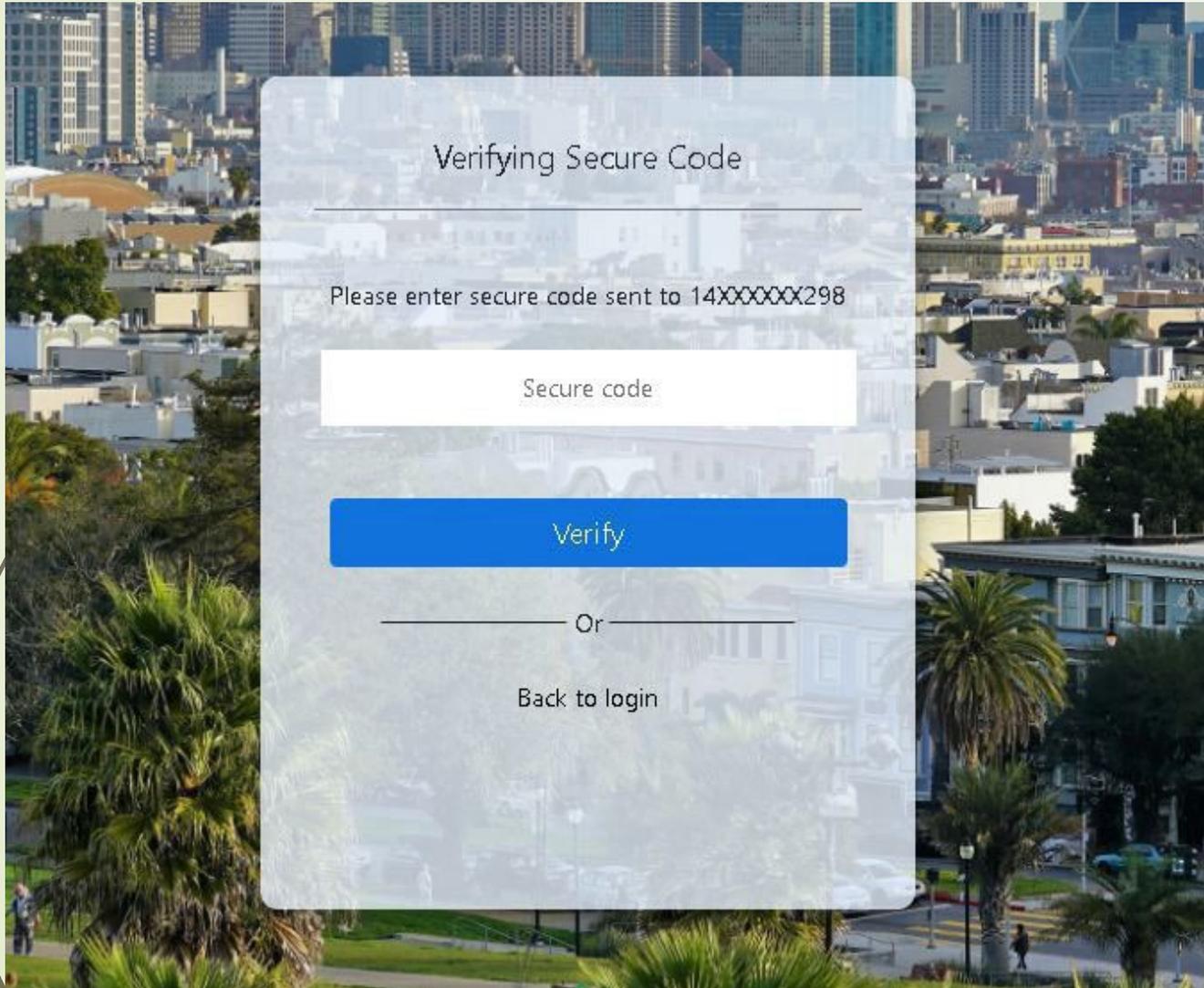
Submit

Or

[Back to login](#)

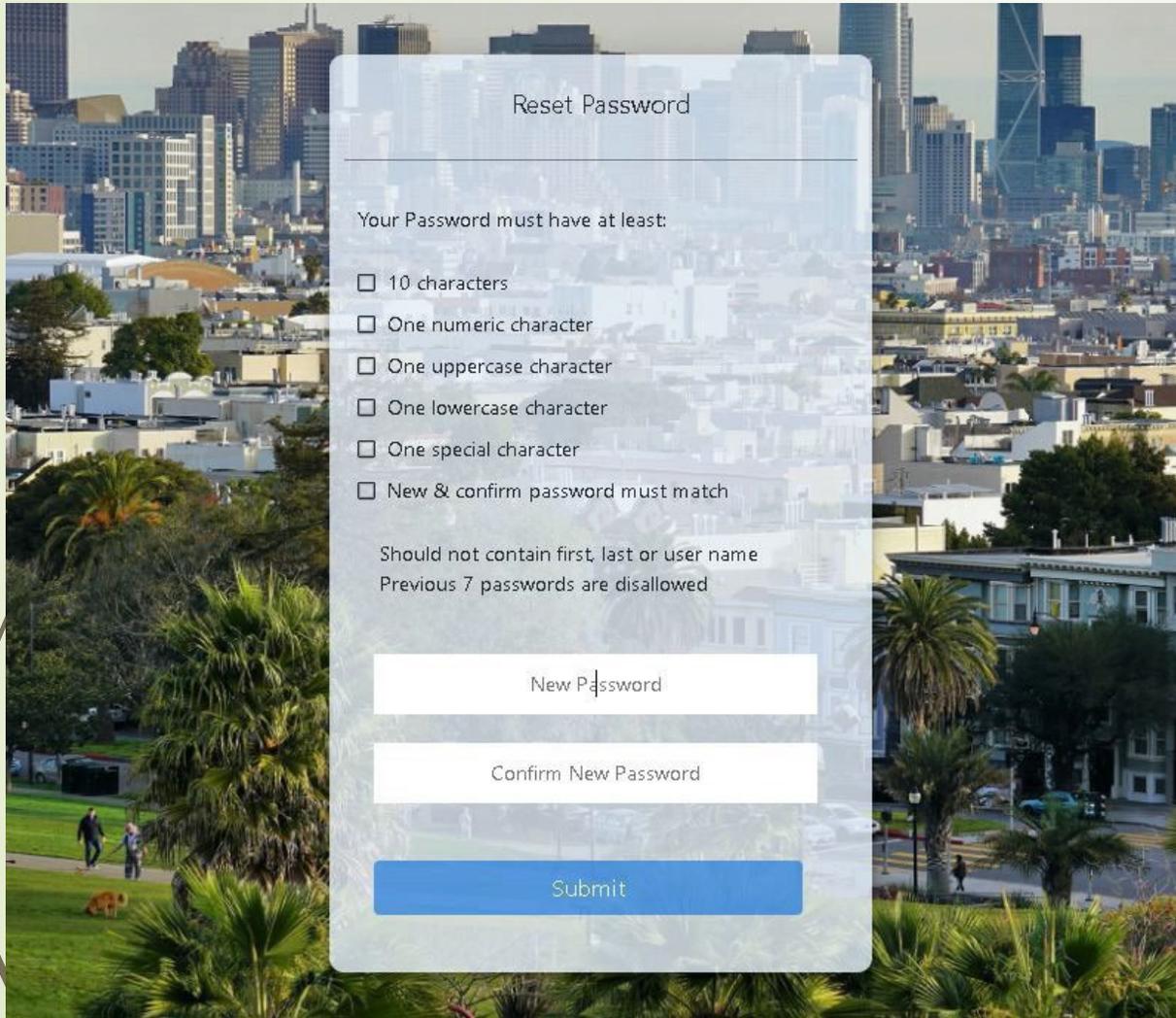
- Enter your UCSF POI#
- Select 'Submit'

Verifying Secure Code Page



- Enter Secure Code from Phone
- Select 'Verify'

Reset Password Page



Reset Password

Your Password must have at least:

- 10 characters
- One numeric character
- One uppercase character
- One lowercase character
- One special character
- New & confirm password must match

Should not contain first, last or user name
Previous 7 passwords are disallowed

New Password

Confirm New Password

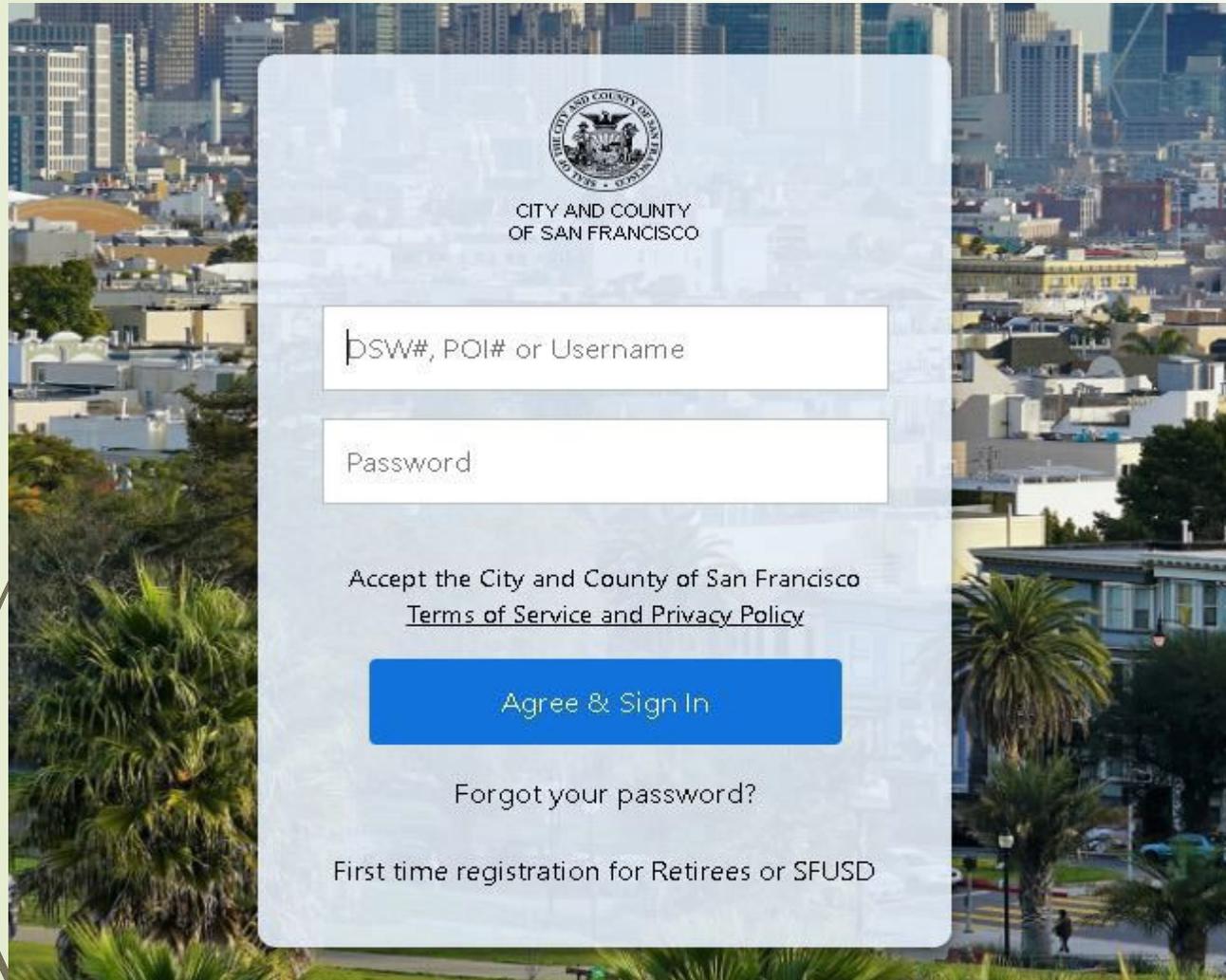
Submit

New Password Guidelines:

- 10 characters
- One numeric character
- One uppercase character
- One lowercase character
- One special character
- New & confirm password mustmatch

Select "Submit"

CCSF Login Page

A screenshot of the CCSF Login Page. The page features a light blue background with a faint cityscape. At the top center is the City and County of San Francisco seal, with the text "CITY AND COUNTY OF SAN FRANCISCO" below it. There are two input fields: the first is labeled "PSW#, POI# or Username" and the second is labeled "Password". Below the input fields is a link for "Terms of Service and Privacy Policy". A blue button labeled "Agree & Sign In" is positioned below the link. At the bottom, there are links for "Forgot your password?" and "First time registration for Retirees or SFUSD".

CITY AND COUNTY OF SAN FRANCISCO

PSW#, POI# or Username

Password

Accept the City and County of San Francisco
[Terms of Service and Privacy Policy](#)

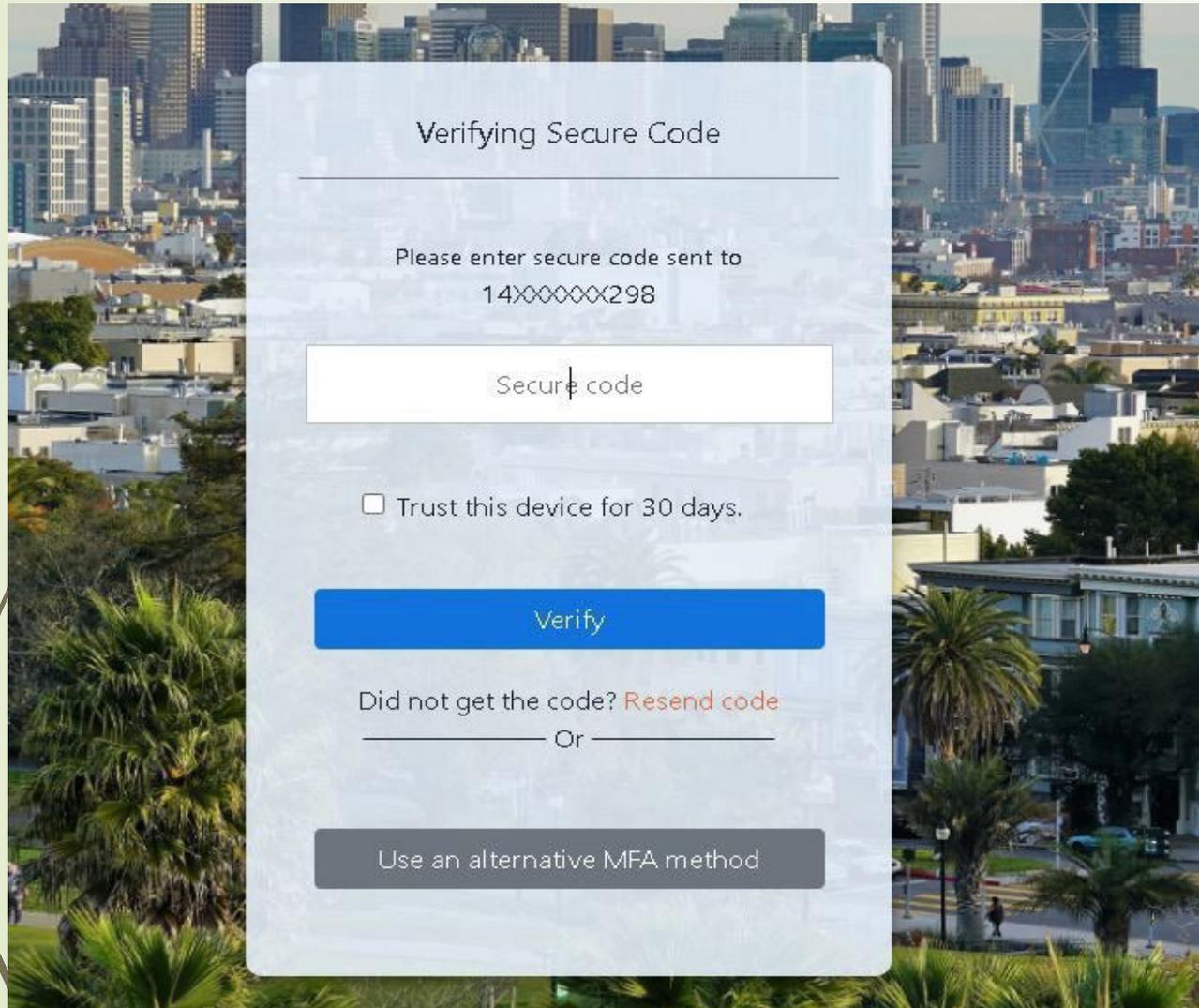
Agree & Sign In

[Forgot your password?](#)

[First time registration for Retirees or SFUSD](#)

- Enter UCSF POI#
- Enter Password
- Select 'Agree & Sign In'

Verifying Secure Code



The screenshot shows a mobile application interface for verifying a secure code. The background is a blurred cityscape. The app window has a light blue header with the title "Verifying Secure Code". Below the header, there is a horizontal line. The main text reads "Please enter secure code sent to 14XXXXXXXX298". Below this is a white input field with a light blue border and the placeholder text "Secure code". Underneath the input field is a checkbox labeled "Trust this device for 30 days.". Below the checkbox is a blue button with the text "Verify". At the bottom of the screen, there is a link that says "Did not get the code? Resend code" followed by "Or" and another link. At the very bottom, there is a grey button with the text "Use an alternative MFA method".

- Enter Secure Code from Phone
- Select 'Trust this device for 30 days'
- Select 'Verify'

CCSF Dashboard Page

If you have logged onto this site previously, you may be directed to Step 22

Select 'Multi-Factor'

(To Add Additional
Layer of Security)

The screenshot shows the CCSF Dashboard Page. At the top, there is a blue header with a home icon, a menu icon, and a notification icon. Below the header, the breadcrumb "Home / Dashboard" is visible. The main content area is titled "Click the application tile you wish to access." and contains a grid of application tiles. A yellow arrow points to the "Multi-Factor" tile, which is not explicitly labeled in the image but is implied by the text on the left. The tiles include:

- Remote Work & MS Teams Training
- MS Teams
- Email and Calendar
- CyberSafeSF
- Advanced Home Security
- SF Employee Portal
- SF Employee Portal Support
- DT ServiceNow
- SF.GOV
- SF SecureShare
- Combined Charities

Multi-Factor Page

User Guide: Register Multi-Factor Authentication (MFA)

The MyApps Portal requires users to set up at least two multi-factor authentication (MFA) methods after validating their login credentials to access their account.

1. Enroll first MFA factor

Go to <https://myapps.sfgov.org/>.

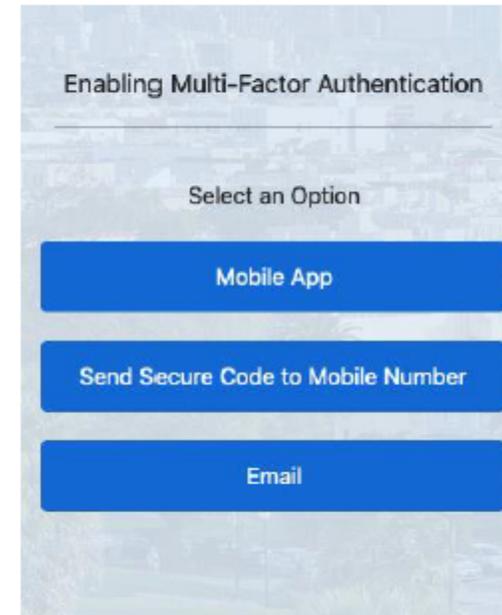
Enter username:

(Employees use DSW number,
POIs use POI number,
Contractors use loginID,
Suppliers use supplierID number)

and password.

Click "Agree & Sign in".

After validating login credentials, the user will see a window that asks to enroll in at least one MFA factor such as Mobile App, SMS to Mobile Number and Email.



Multi-Factor Page (continued)

1.1 Enroll Mobile Number

- Click "Send Secure Code to Mobile Number" button.
- Then, it will open a new window where a user must enter a mobile number and click "Enroll" button to receive a mobile message with a secure code.

- Enter the secure code that you received on your mobile number and click the "Verify" button to complete the enrollment of mobile number as shown in the image:

- Click the "Done" button to get access to the account or click "enroll other factors" to setup others such as email or mobile app.

Multi-Factor Page (continued)

1.2 Enroll Mobile App

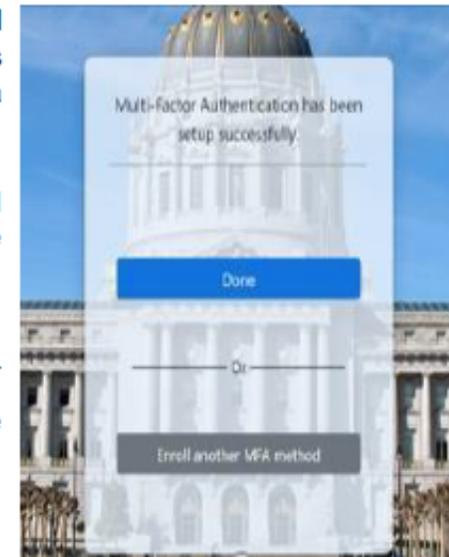
- Click the "Mobile App Notification" button.

Note: Download the Oracle Authentication Mobile App from the iOS App Store or Google Play Store.

- After clicking "mobile app notification", a user will see a screen with QR code to scan as shown:
- Once the app is installed on your phone, open the camera from the Oracle Authenticator app and scan or hover the camera over the QR code as showing in the below image.



- After the QR code has been scanned, you will be asked to add a new device or overwrite an existing one. If this is your first time setting up the app, please select add a new device.
- After the mobile application has been installed and configured on your mobile device, you will see the following screen on your computer:
- Click the "Done" button to get access to the account or click "enroll other factors" to setup email or a mobile phone.



Multi-Factor Page (continued)

1.3 Enroll Email

- Click "Email" button.
- A new window opens and asks the user to enter the One Time Passcode (OTP) sent to their email.
- Enter the One Time Passcode (OTP) that you received on your email and click the "Verify" button to complete the enrollment of email as shown in the image.
- Click the "Done" button to get access to the account or click "enroll other factors" to setup others such as email or mobile app.

Verifying Email Secure Code

Please enter secure code sent to [redacted]@sfgov.org

456706

Verify

Did not get the code? [Resend code](#)

Or

Enroll another MFA method

Multi-Factor Page (continued)

2. Enroll second MFA factor

Users are allowed to add multiple Mobile App, SMS, and FIDO authentication factors; however, they can add only one email factor.

To add a new MFA factor, click "Configure" on the tile or click the arrow on the MFA menu  and choose one of 'Add FIDO Authenticator', 'Add Mobile App', 'Add Mobile Number'.

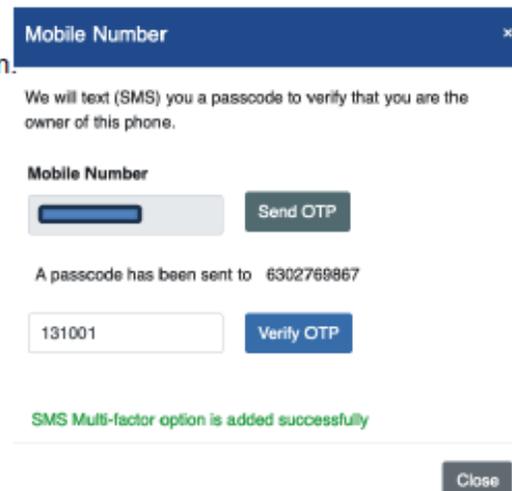
2.1 Enroll Mobile Number

To add a new Mobile Number (SMS Factor)

- Click 'Configure' on the Mobile Number tile or click 'Add Mobile Number' menu from the MFA menu (burger)
- On the pop-up window enter the mobile number you wish to enroll, then click **Send OTP** button.



- On the next page, enter the One Time Passcode received on your mobile and click **Verify OTP** button. The message "SMS Multi-factor option is added successfully" will be displayed.



Multi-Factor Page (continued)



- Click 'Configure' on the Mobile App tile or click 'Add Mobile App' from the MFA menu (burger)
- Note: Users can download the Oracle Authentication mobile app from the mobile iOS App Store or Google Play Store.



- A pop-up box will appear in the middle of the screen as shown below:
- Once the app is installed on their phone, users can open the camera from the Oracle Authenticator app and scan or hover the camera over the QR code (shown in the image below).

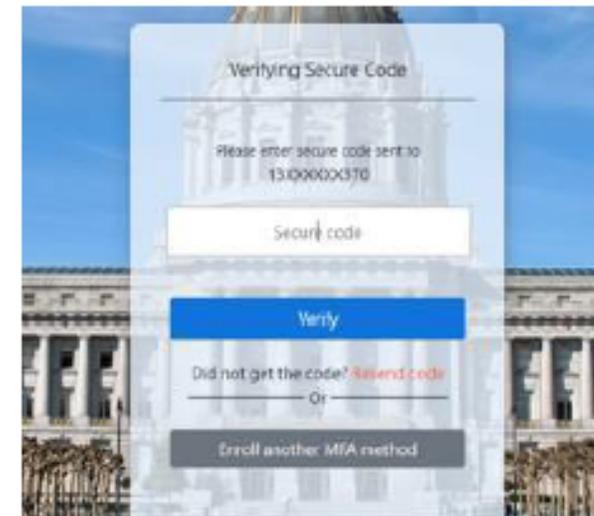
2.3 Enroll Mobile App

- Once users scan the QR code, a pop-up box will appear on their mobile screen, asking them to add a new device or overwrite the existing one. If using the authenticator app for the first time, users should select "add new." Otherwise, users can select "overwrite."
- Once the QR code has been scanned in the authenticator app and configuration is done, select "close" to see the enrolled device info in the mobile app section.

3. Authenticate using MFA to access the MyApps Portal

After enrolling in MFA users will need to authenticate using MFA to gain access to the MyApps Portal.

- If a user has set email authentication as their default, they will see the following screen.
- The user should follow the instructions on screen to enter the secure passcode received by email.
- Click the "Verify" button. The user will be redirected to the MyApps Portal dashboard.



Step 16

- If a user has set mobile number authentication as their default, they will see the following screen.

- The user should follow the instructions on screen to enter the secure passcode received by their mobile device.

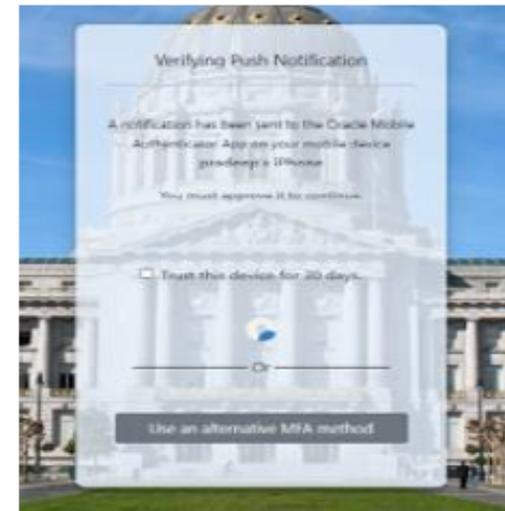
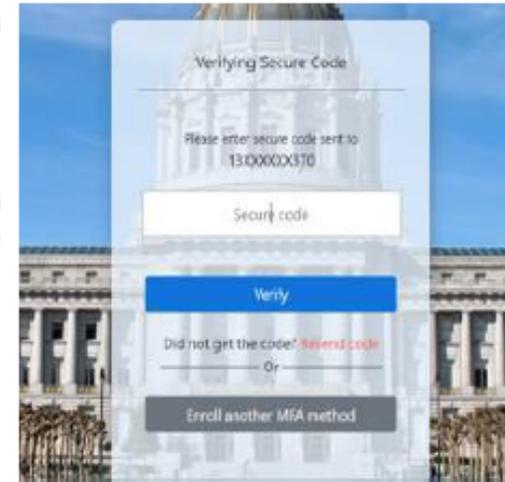
- Click the "Verify" button. The user will be redirected to the MyApps Portal dashboard.

- If a user has set mobile app authentication as their default, they will see the following screen.

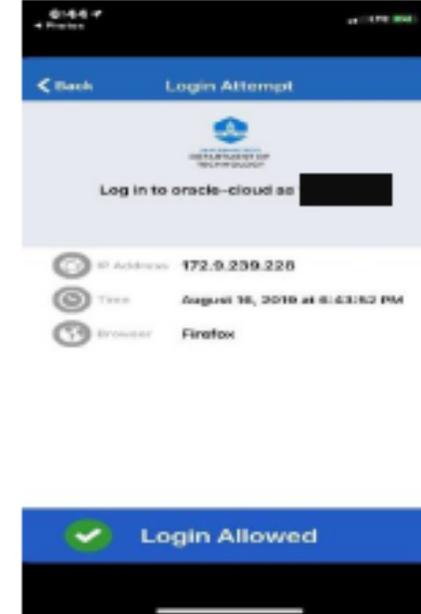
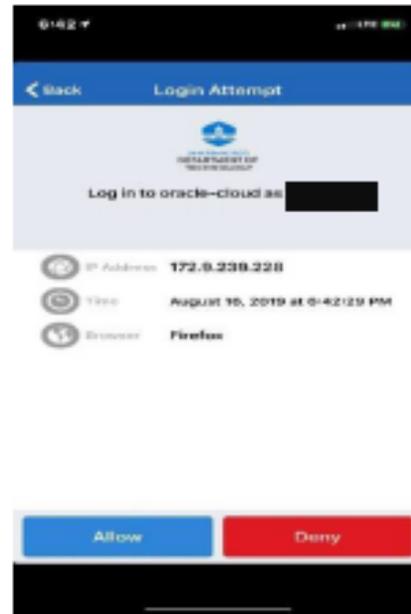
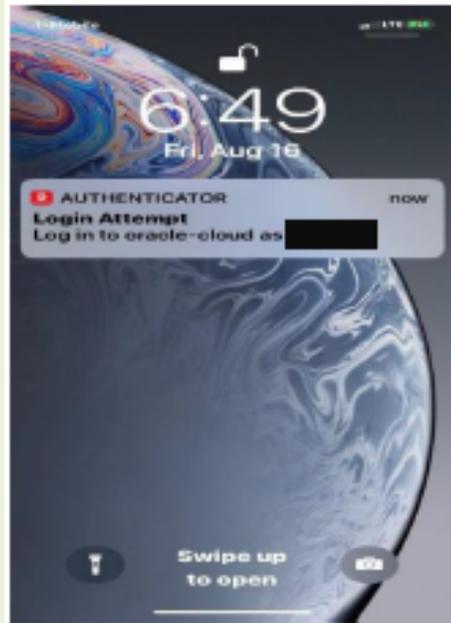
- The user should follow the instructions on screen to approve the push notification received by their mobile device.

- Open the push notification in the "Oracle Authentication App" on the user's mobile device.

- Tap the "Allow" button on the mobile device. After few seconds, the user will be redirected to the MyApps Portal dashboard.

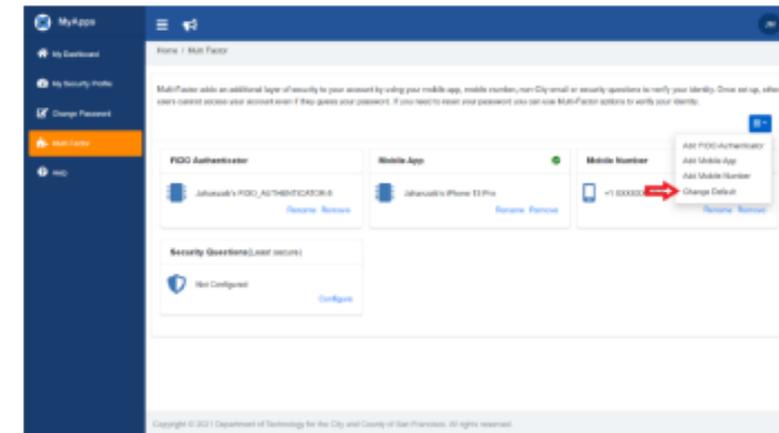
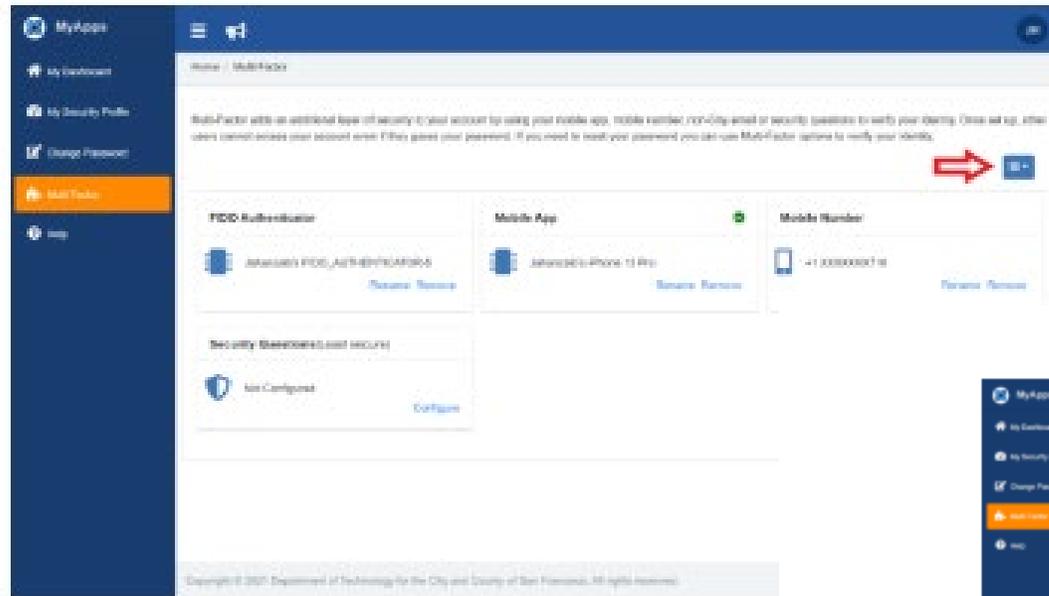


Step 17



- A user can also check the box "Trust this device for 30 days" to prevent MFA verification each time a user access MyApps portal.

4. Set default MFA Factors



- This feature helps a user to choose which MFA factor they want to use for authentication when accessing the MyApps Portal from an external network.
- Click the “Change Default” button.

Step 19

- After clicking the “Change Default” button, a new pop-up screen will appear as shown:

Change default MFA

Select your default 2-Step Verification method.

- FIDO Device** Jahanzaib's FIDO_AUTHENTICATOR-5
- Mobile App Notification** Jahanzaib's iPhone 13 Pro
- Mobile App Passcode** Jahanzaib's iPhone 13 Pro
- SMS Text Message** +1 XXXXXXXX718

Set as Default Cancel

- Users can select an MFA factor such as Email, Mobile Number, Mobile App or FIDO Device by choosing a radio button from the list.
- Once a radio button is selected, click the “**Set as Default**” button.

5. Remove MFA Factors such as Security Questions, Mobile Number and Mobile App



- Users should select the MFA factor they want to remove such as Email, Mobile Number or Mobile App. For example, if they want to remove an email MFA factor, they can go to the email section and click the “Remove” button on the right side of the pane as shown in the image.



- After clicking “remove”, you will see a pop-up box that will ask you to confirm your selection again.

CCSF Dashboard Page

The screenshot shows the CCSF MyApps dashboard. On the left is a dark blue sidebar with the 'MyApps' logo and a list of links: 'My Dashboard' (highlighted in orange), 'Change Password', 'Multi Factor', and 'Help'. A red arrow points to the 'My Dashboard' link. The main content area has a blue header with a hamburger menu and a megaphone icon. Below the header, it says 'Home / Dashboard' and 'Click the application tile you wish to access.' There are ten application tiles arranged in two rows of five. The top row includes: 'Remote Work & MS Teams Training' (house icon), 'MS Teams' (T icon), 'Email and Calendar' (envelope icon), 'CyberSafeSF' (shield icon), and 'Advanced Home Security' (Z icon). The bottom row includes: 'SF Employee Portal Support' (purple building icon), 'DT ServiceNow' (now logo), 'SF.GOV' (seal icon), 'SF SecureShare' (lock icon), and 'Combined Charities' (heart icon). A yellow arrow points to the 'SF Employee Portal' tile in the top row.

Choose 'SF Employee Portal'

SF Employee Portal

SF EMPLOYEE PORTAL

HOME SIGNOUT

HOME EMERGENCY RESPONSE USER ACCESS & SUPPORT FAVORITES

MY INFORMATION MY PAY MY TIME MY BENEFITS MY LEARNING MY LINKS

Anne Shirley
IS Business Analyst-Principal
Period: 07/25/2020 - 08/07/2020 Select: Current Update

Scheduled: 80.00 Hours Reported to Date: 80.00 Hours Approved: No

Day	Type	Status	Sub-Total	Total
Saturday 07/25/2020			0.00	
Sunday 07/26/2020			0.00	
Monday 07/27/2020	Regular Hours - Worked	Scheduled	8.00	8.00
Tuesday 07/28/2020	Regular Hours - Worked	Scheduled	8.00	8.00
Wednesday 07/29/2020	Regular Hours - Worked	Scheduled	8.00	8.00
Thursday 07/30/2020	Regular Hours - Worked	Scheduled	8.00	8.00
Friday 07/31/2020	Regular Hours - Worked	Scheduled	8.00	8.00

VIEW NEWS ARCHIVE

MY LINKS ALERTS MY TO-DOS

WORK LINKS EMPLOYEE LINKS

SF LEARNING SF OPEN BOOK

DO NOT Select 'My Learning' option



Select 'WorkLinks'

then

Select 'SF Learning'

SF Learning Platform Page



Select 'My Learning'

My Learning Requirements Portal: **Current**

The screenshot shows the 'My Learning' portal interface. On the left is a navigation sidebar with a 'My Learning' menu item highlighted. The main content area has tabs for 'Current', 'Planned', and 'History', with 'Current' selected. Below the tabs is a 'Current Learning' section containing a list of training modules. The first module is 'Cybersecurity Training', which is a 'Web-based Training' and is 'Enrolled'. A 'Launch' button is visible at the bottom of the module card. A yellow arrow points to the title 'Cybersecurity Training'.

#1

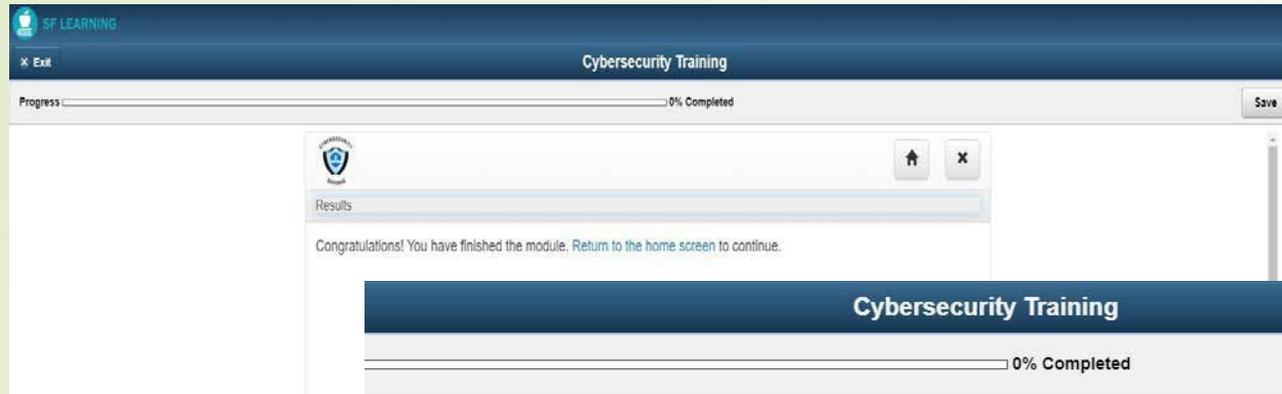
#2

#3

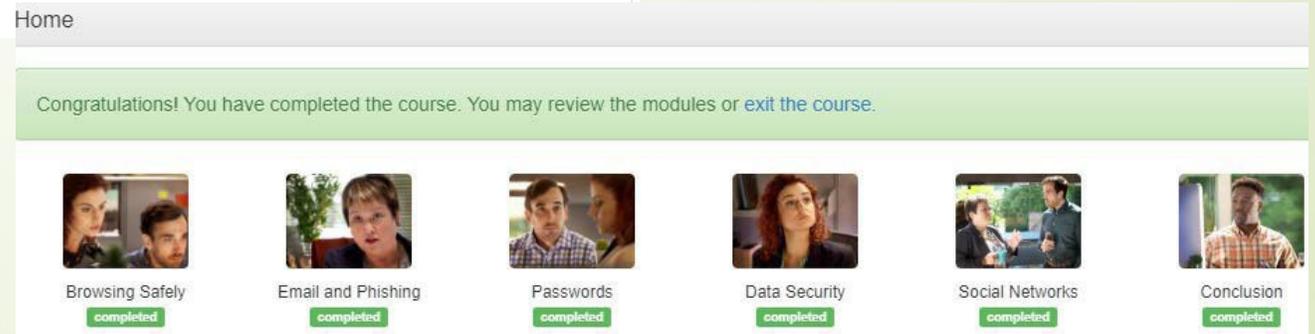
Arrows #1, #2, and #3: Ensures you are in the 'Current' Tab of the 'My Learning' section to view all required trainings and to select 'Launch' to start a training.

Select the title of the module to start a requirement. Do NOT select 'Launch'

Recommended: Take Screenshots



Helpful Tip:
Take screenshots when completing a module & requirement, in case the system does not automatically record completion.



My Learning Requirements Portal: **History**

The screenshot displays the 'My Learning' portal interface. On the left, a navigation menu includes 'My Learning', 'Certification Status', 'Learning Plans', and 'Add Supplemental Learning'. The 'My Learning' tab is selected, indicated by arrow #1. The main content area features three tabs: 'Current', 'Planned', and 'History'. The 'History' tab is active, indicated by arrow #2. Below the tabs, the 'Learning History' section shows a list of completed training items. The first item is 'Cybersecurity Training', which is a 'Web-based Training' completed on 24 Aug 2020. This item has 'Launch' and 'Print' buttons. The second item is 'DPH Annual Compliance and Priv...', also a 'Web-based Training' completed on 05 Feb 2020, with 'Launch' and 'Print' buttons. The third item is 'ZSFG General Orientation', a 'Classroom' training completed on 23 Dec 2019, with a 'Print' button. Arrow #3 points to the 'History' tab.

Arrows #1, #2, and #3: Ensures you are in the 'History' Tab of the 'My Learning' section to verify the system recognizes completion of the Cybersecurity Training.

Congratulations!

**You have successfully logged into the SF Employee Portal,
launched the My Learning application, and completed the
Annual Cybersecurity training!**



THANK
YOU!