Public Safety Report System (PSRS)
Getting Started Step by Step

Contents

Before Starting Account Registration:

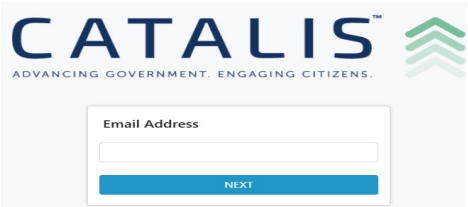
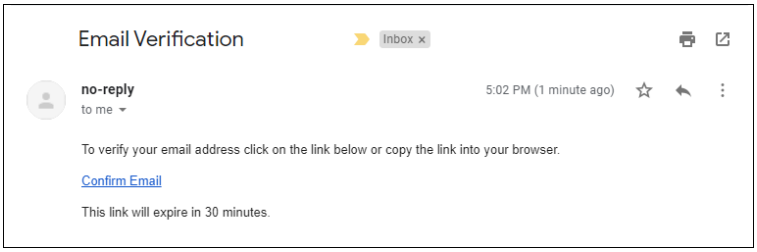
Ensure you have:

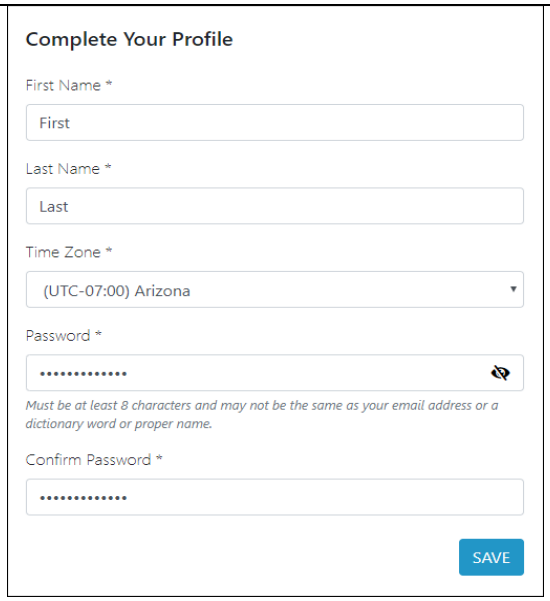
- Access to your work email account
- A mobile device if using an authenticator app
- Approximately 10–15 minutes to complete setup
- The ability to complete the process in one session

> **Pro Tip:** Complete the following steps in one session. If you begin this process and exit before finishing, your account may be locked and require a reset OCA.

Initial Profile and Multifactor Authentication Set Up:

Step	Instructions
1.	If your job duties require access to the Public Safety Report System (PSRS), contact your Local Administrative User (LAU) to request access. The **LAU will create your user profile** within the PSRS and assign the appropriate permissions based on your job responsibilities. During setup, the LAU will enter your: • Name

	• Work email address (personal email accounts such as Gmail, Yahoo, AOL, etc. should not be used.) *If your location does not have an official county, city, state, or government email domain, contact the Bail and Pretrial Team at bail@txcourts.gov for assistance*. • Job title • DPS issued TLETS User ID (when applicable) • Assigned location(s) • Appropriate system permissions and access levels ** If you are unsure who your Local Administrative User (LAU) is, email bail@txcourts.gov and include your agency, city and county.*
2.	Once your account has been created by your LAU, they will notify you with instructions for completing your account registration. Open a web browser and **navigate to** https://bail.txcourts.gov. **Pro Tip**: Bookmark the website for quick and easy access in the future.
3.	From the login screen, enter your email address and click **NEXT.** 
4.	The system will send a verification link to the email address you provided. Follow the instructions to verify the email address.  *If you are unable to proceed because the system does not recognize your email address: ensure your LAU has completed the set-up process and the email entered is correct. If the email entered was not correct, you will need to email bail@txcourts.gov requesting your email address be updated.*
5.	After you verify your email address, complete your profile by filling in each required field: Name, Time Zone. Choose the appropriate time zone where you normally perform your work duties (*do not skip this step, as it will cause log-in issues later*), and create a password. Then click **Save**.

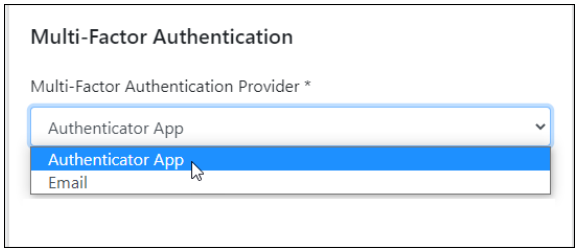


6. Setting up Multi-Factor Authentication (MFA) is required. The authenticator can be configured to verify your login using either your mobile device or your work email address. *(Phone verification – see step 7, Email verification – see step 8)*

When selecting your MFA method, consider which option will be the most accessible during your normal workday. If you work in a secure facility or location where cellular phones are restricted, an authenticator application on your mobile device may not be readily available, and email authentication may be a better option.

*Keep in mind that you will need access to your selected authentication method each time you log in to the PSRS. If you change email addresses, *replace your mobile device, or remove the authenticator application, you may need assistance resetting your MFA settings.*

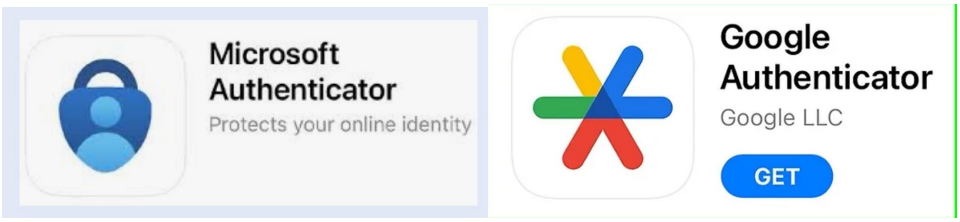
**If you replace your mobile device, review the steps outlined in section titled 'Resetting MFA for a New Phone'.*



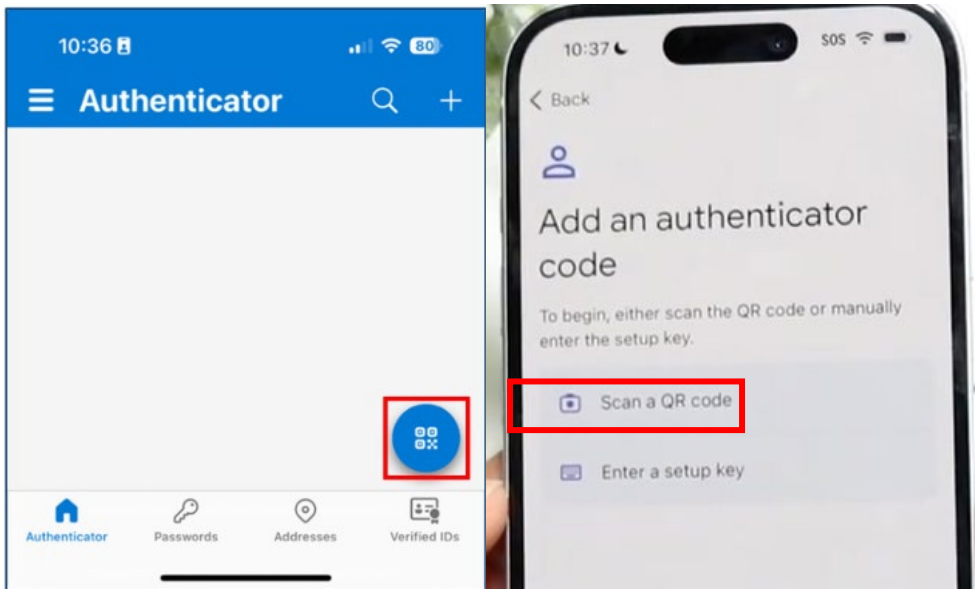
Proceed to Step 7 if you selected Authenticator App, or Step 8 if you selected Email.

7. **Cellular Phone Authentication App Instructions** *(email Authentication steps are located in Step 8.)*

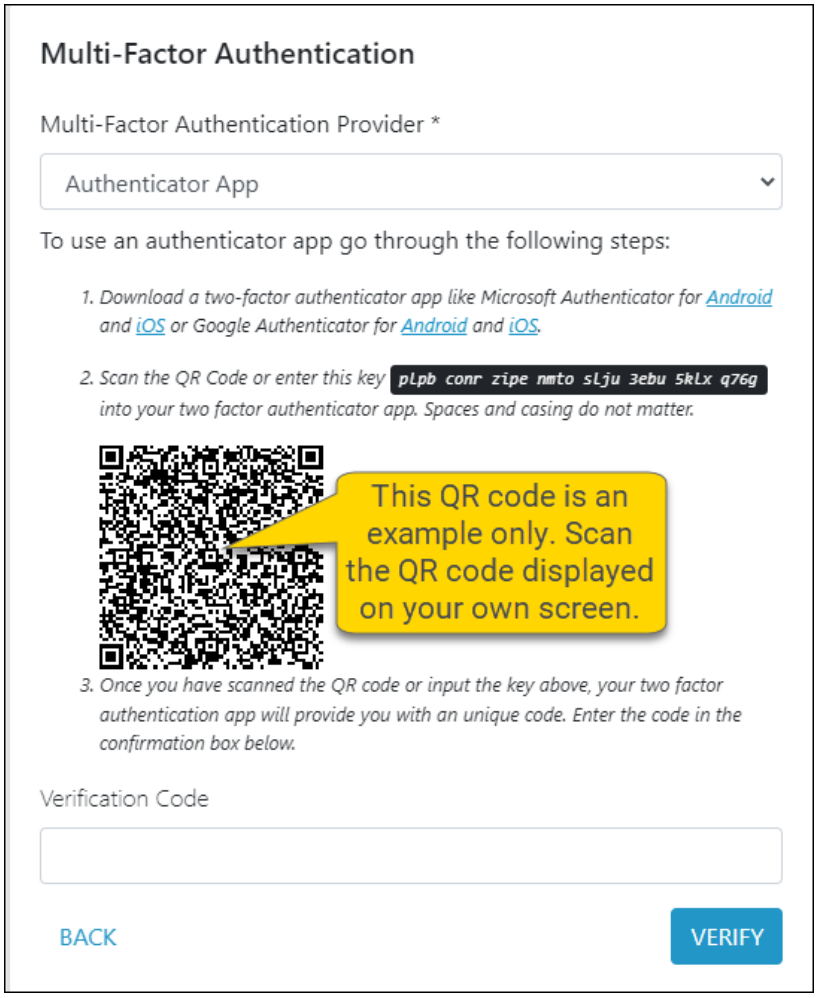
7a. Download either the **Microsoft Authenticato**r app or the **Google Authenticator** app from the Apple App Store or Google Play Store. *If you attempt to use a different authenticator app, you may be prompted to purchase a subscription or create an account. These additional services are not required to access the PSRS.*



7b. Open the authenticator application on your mobile device. Select the QR code reader within the application (see examples below). Your phone's camera will open automatically. Hold your phone over the QR code displayed on the PSRS registration screen until the code is successfully scanned.



Microsoft Authenticator **Google Authenticator**



7c. Once the QR code has been scanned, the authenticator application will create an account labeled **Catalis Identity Server** and begin generating a unique six-digit verification code. Enter the verification code when prompted during the PSRS login process to complete authentication.

Important: You will be prompted to use the authenticator application each time you log in to the PSRS. The six-digit verification code changes automatically every 30–60 seconds for security purposes.

Removing the authenticator application from your device or deleting the **Catalis Identity Server** account may prevent you from accessing the PSRS until your authentication settings are reset.

Troubleshooting

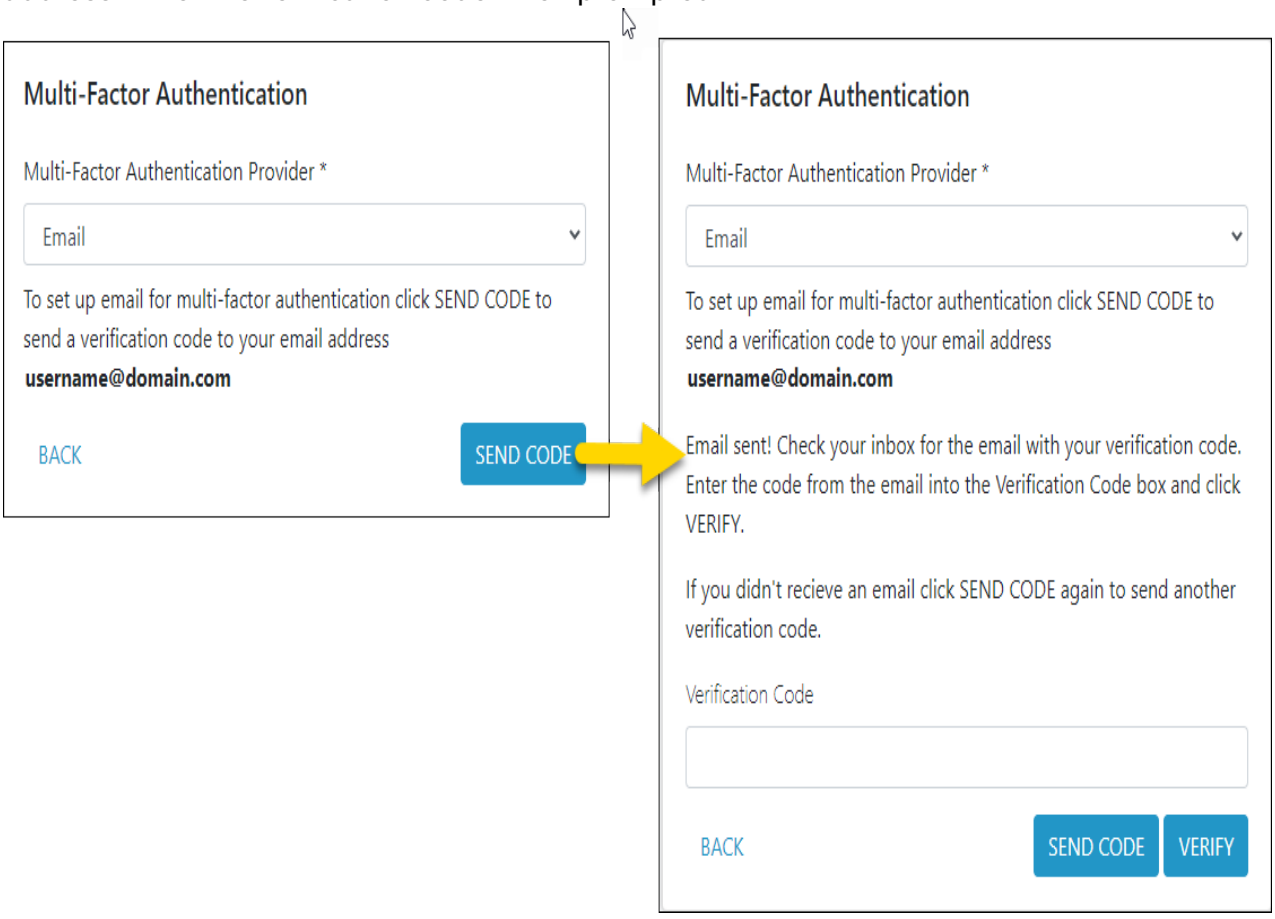
If you experience issues with authentication, verify the following:

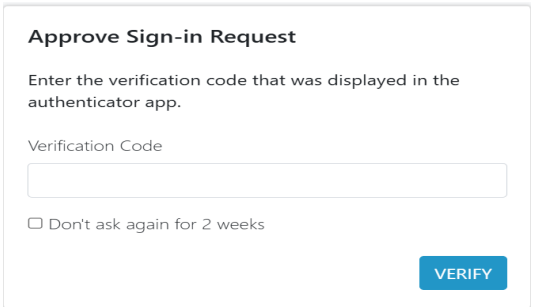
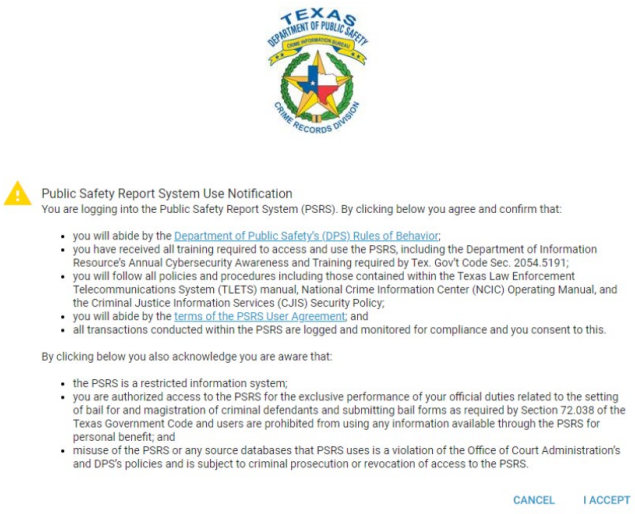
- Your computer and mobile device are displaying the correct date and time.
- Automatic date and time synchronization is enabled on your mobile device, if available.
- The QR code was successfully scanned, and the **Catalis Identity Server** account appears within your authenticator application.
- You are entering the current six-digit verification code before it expires.

If you continue to experience issues, contact your Local Administrative User (LAU) or the Bail and Pretrial Team for assistance.

8. **Email Authentication Instructions**

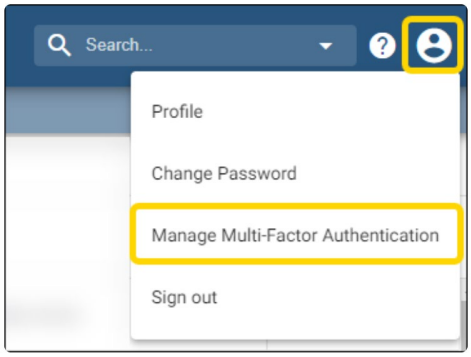
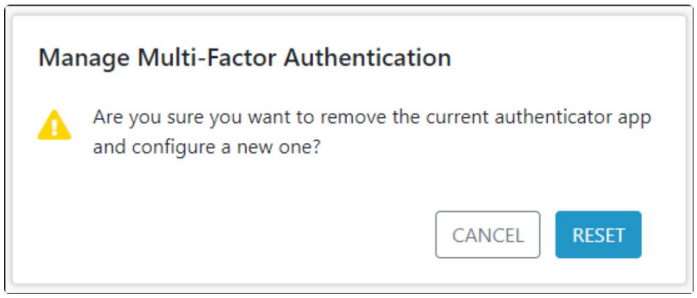
8a. Continue following the on-screen instructions to send a **verification code to your email** address. Enter the verification code when prompted.



	Pro Tip: The registration email is typically delivered within a few minutes. If you do not receive it, check your spam or junk folder before contacting your LAU or Bail@txcourts.gov.
9.	Follow the prompts to enter your verification code from your email or cell phone. **Pro Tip:** While MFA is generally required each time you log in, if you check the box 'Don't Ask again for 2 weeks', performing the MFA steps will not be required for any subsequent logins over the next 2 weeks.  9a After setting up multi-factor authentication, you may see a screen displaying the message **"No Products Found."** Click the menu icon in the upper-left corner of the screen and select **TAIMS**. If you receive the **"No Products Found"** message and do not see the **TAIMS** option after selecting the menu icon, submit a support request to Catalis at support@automon.com 
10.	The **PSRS Use Notification** page appears. Review the notification and click **I Accept** to continue. By selecting **I Accept**, you acknowledge and agree to comply with the DPS Rules of Behavior, which can be accessed through the hyperlink provided on the page *(Rules of Behavior are also included in this document in the appendix section.)* 
11.	The PSRS home page appears. Your account registration is complete, and you are ready to begin using the Public Safety Report System

Updating Your MFA Preference:

Utilize these instructions if you need to switch your MFA from email to cell phone or vice versa. If you get a **new phone**, follow step 3-4 in this section.

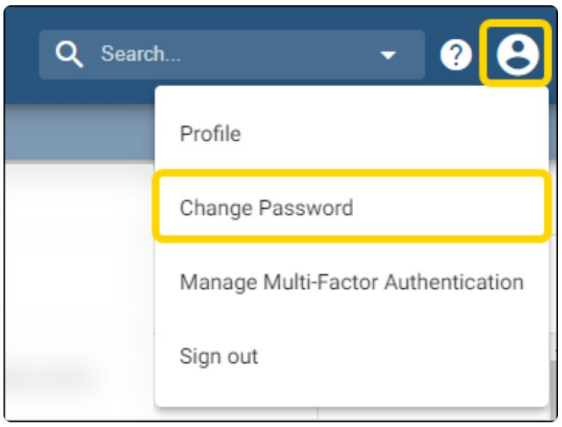
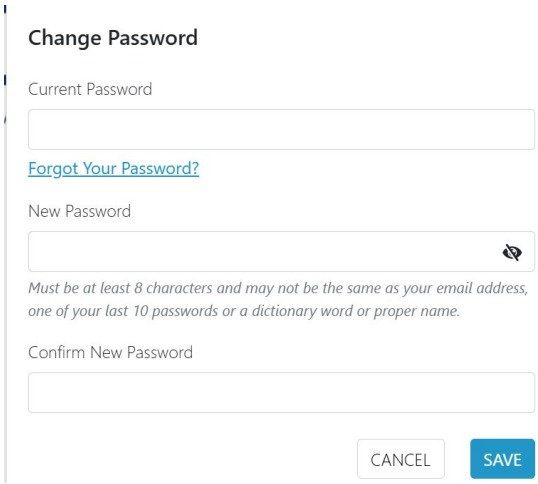
Step	Instructions
1.	Once you have signed into the PSRS, click on the profile icon at the top right-hand side of the landing page and click on **Manage Multi-Factor Authentication.** 
2.	Click on **Reset** when prompted. 

Resetting MFA for a New Phone:

1.	Contact OCA by sending an email to bail@txcourts.gov requesting that your MFA be reset.
2.	Once you have received confirmation from the Bail & Pretrial Team that your MFA has been reset continue with Steps 7-9 in the 'Initial Profile and Multifactor Authentication Set Up' above.

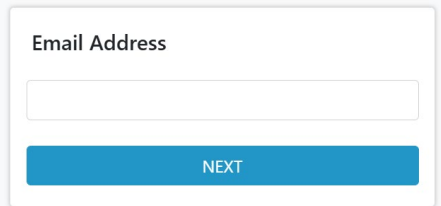
Updating and Changing Your Password:

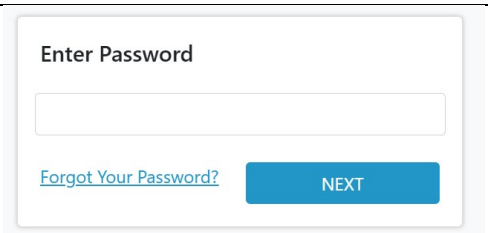
For security and CJIS compliance, the PSRS prompts you to change your password every 90 days. Additionally, you are able to change your password at any other time by completing the steps below. Password requirements are displayed on-screen during setup. *If you have been locked out for attempting to enter your password incorrectly too many times, skip to the next section "Locked out of PSRS for Password Error Entry".*

Step	Instructions
1.	Once you have signed into the PSRS, click on the profile icon at the top right-hand side of the landing page and click on **Change Password**. 
2.	Follow the prompts in each field to reset the password. 
3.	Click on **Save.** You have successfully changed your password.

Locked out of PSRS for Password Error Entry

Pro Tip: The PSRS resets itself five minutes after your last attempted log in. Therefore, if you are locked out, wait the allotted time and attempt to login again.

1.	If you have forgotten your password, enter your email address as prompted during log in. Click **NEXT.** 
2.	Click on **Forgot Your Password,** and follow the prompts to reset your password.

Updating Your Email Address:

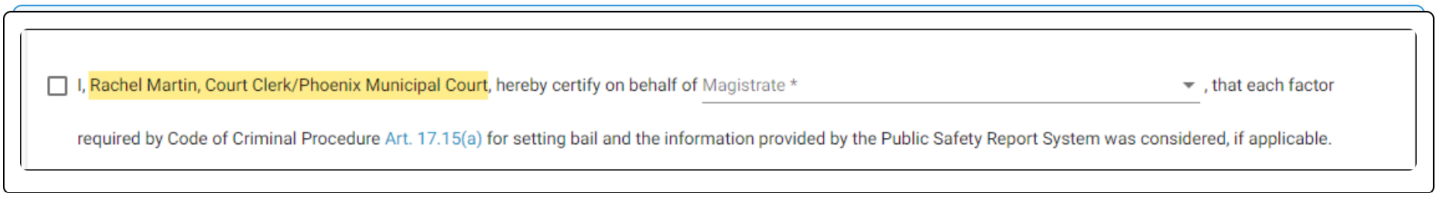
Email addresses associated with PSRS user accounts can only be updated by the Office of Court Administration (OCA). Do not create a new PSRS account if your email address changes. Contact OCA so your existing account can be updated.

PSRS accounts must be associated with an official government, court, county, city, state, or agency-issued email address. Personal email accounts (such as Gmail, Yahoo, AOL, Outlook.com, etc.) may not be used.

If your work email address changes, contact the Bail and Pretrial Team at bail@txcourts.gov and provide your name, agency, previous email address, and new work-issued email address. OCA will update your account and provide any additional instructions necessary to restore access.

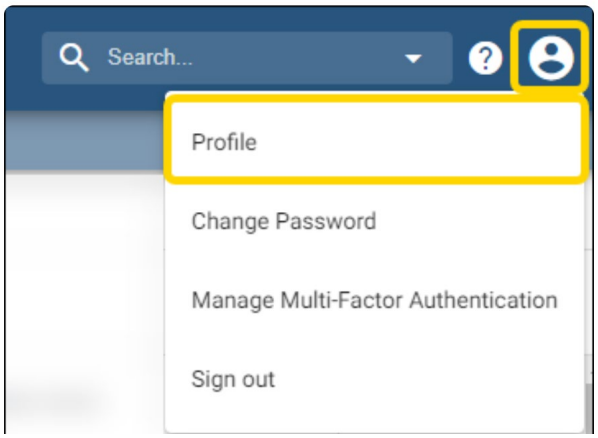
Updating Your Profile:

The LAU will enter your position and office when setting up your account. However, if you have permissions to certify the electronic Bail Form (either as a magistrate or on behalf of a magistrate), the certification statement populates the name, position and office shown in your profile.



If this was set up incorrectly or needs to be updated, follow the instructions below:

Step	Instructions
1.	Once you have signed into the PSRS, click on the profile icon  at the top right-hand side of the landing page and click on **Profile**.

	
2.	In the dialog box, make the necessary updates to your name, position, and/or office. 

Appendix:

DPS Rules of Behavior for Individuals Accessing DPS Data (see full document, next page):

1. I understand that I am required to perform my official duties when given access to DPS data.
2. I must restrict disclosure of DPS data to only those with a business need, and are authorized to receive the information.
3. I must not send or store DPS sensitive or confidential information to a personal e-mail account.
4. I must take every precaution to prevent unauthorized individuals from observing display output. (Use privacy screens, keep computer screens from facing windows or doors, etc.)
5. I must log off or lock my workstation or laptop computer, or I must use a password-protected screensaver, whenever I step away from my work area, even for a short time.
6. I must not transmit DPS sensitive or confidential information unencrypted outside the secure network.
7. I must securely store all removable media containing DPS data when not in use.
8. I will ensure DPS sensitive or confidential data stored on removable or portable media is AES 256 encrypted, and the media is marked with the appropriate data classification.
9. I will comply with the DPS password policy.
10. I will immediately report security violations, and incidents involving DPS data to my supervisor and DPS Cyber Security.

Department of Public Safety
Cyber Security Unit
Austin, TX 78752
10/15/2020

Rules of Behavior for Individuals Accessing DPS Data

Purpose

This document delineates the responsibilities and expected behavior of all individuals that use and have access to data provided by the Department of Public Safety of the State of Texas (DPS). Additionally, this document fosters the comprehensive knowledge of and compliance with the DPS rules of behavior as a condition for continued data access and sets forth requirements for verification of understanding with the rules as documented. DPS data users will be held accountable for their actions and are responsible for securing the data and resources in accordance with the DPS rules of behavior. All persons requiring access to DPS data must read, understand, and formally acknowledge those rules of behavior by signing this agreement prior to being granted access to DPS data.

User Rules of Behavior

1. I understand that I am required to perform my official duties when given access to DPS data.
2. I must restrict disclosure of DPS data to only those with a business need, and are authorized to receive the information.
3. I must not send or store DPS sensitive or confidential information to a personal e-mail account.
4. I must take every precaution to prevent unauthorized individuals from observing display output. (Use privacy screens, keep computer screens from facing windows or doors, etc.)
5. I must log off or lock my workstation or laptop computer, or I must use a password-protected screensaver, whenever I step away from my work area, even for a short time.
6. I must not transmit DPS sensitive or confidential information unencrypted outside the secure network.
7. I must securely store all removable media containing DPS data when not in use.
8. I will ensure DPS sensitive or confidential data stored on removable or portable media is AES 256 encrypted, and the media is marked with the appropriate data classification.
9. I will comply with the DPS password policy.
10. I will immediately report security violations, and incidents involving DPS data to my supervisor and DPS Cyber Security.

Acknowledgement

I have read and received a copy of the signed (check the box that applies to you):

☐ Data Sharing Agreement (DSA) signed by Department of Public Safety and Entity.

☐ Interconnection Security Agreement (ISA) signed by Department of Public Safety and Entity.

I acknowledge that I have read, and understand the Rules of Behavior and must comply with them.

Name of User (printed):_____

Supervisor's Name: _____

_____ _____

(Applicant Signature) (Date)