

1. **New User Registration:** A new user wants to sign up on the website using a graphical password. They will be prompted to select an image and mark specific points on the image to create their password.
2. **Forgotten Password:** An existing user forgets their password and wants to reset it using their graphical password. They will need to provide the image they previously selected and correctly mark the points to reset their password.
3. **Login Attempts:** An existing user tries to log in to the website several times but fails due to incorrect password marks. They will be prompted to try again or reset their password if they have forgotten it.
4. **Login Success:** An existing user logs in successfully using their graphical password. They will be taken to their account dashboard where they can access their information and perform various actions.
5. **Update Password:** An existing user wants to update their graphical password for increased security. They will be prompted to select a new image and mark specific points to create a new password.
6. **Multiple Devices:** An existing user wants to log in to the website from multiple devices such as a laptop, smartphone, and tablet. They will be able to use the same graphical password on all devices.
7. **Incorrect Password:** An existing user tries to log in with an incorrect password by marking the wrong points on the image. They will be prompted to try again or reset their password if they have forgotten it.
8. **Incomplete Password:** An existing user tries to log in but fails to mark enough points on the image. They will be prompted to try again and mark the required number of points on the image.
9. **Security Measures:** The website implements security measures such as tracking login attempts and temporary lockouts to prevent unauthorized access.
10. **Account Management:** An existing user wants to manage their account information such as their name, email address, and password. They will be able to do so from the account dashboard.
11. **Mobile Login:** An existing user wants to log in to the website from their mobile device. They will be able to do so using their graphical password.
12. **Integration with Other Services:** The website integrates with other services such as social media, email, and cloud storage. An existing user will be able to access these services from their account dashboard using their graphical password.

Use Case no: 1 Use Case Name: Successful New Customer Sign Up

Actors: New Customer

Description: Customer is newly employed at a large firm. Once given their employer-based email they will use that credential to gain access to the site. User will first encounter home page with options to sign up or login for returning users. The new user will click sign in and be taken to the profile creation page. Here the user inputs the email given by the company and then enter fields for name and a text password and create the graphical password as well as establish security questions in the event of needing to recover access. Once finalized a confirmation email is sent containing a link to log back in. Once the link is clicked and identity is confirmed the new user is routed to the home page and can click the login button. The user will enter the email and the text password as well as the graphical password and at this point they will gain access to the work environment.

Alternate Path: Customer can click login and the login page will offer a button for creating a new account if they do not have an existing one.

Pre-condition: Customer must have employer-based email.

Use Case no: 2 Use Case Name: Existing Customer Forgets Password

Actors: Existing Customer

Description: Customer arrives to home page and goes to login as an existing user. Upon being prompted to enter username and password they are rejected entry. Customers will be allowed 3 attempts to gain access to their sensitive data. If the attempts are exhausted, they will be locked out and a recovery email will be sent to the company address. The email will contain a link to recover access. The user will click the link and be taken to the recovery page. Here they must enter their username and answer 3 security questions to regain access to their account.

Alternate Path: Customer can after one failed attempt click a button for "Forgot Password" and the recovery process can begin then. Customers are assumed to know their username as it will be provided by their employer.

Pre-condition: This customer is an existing user and has already established their credentials with the site.

Use Case no: 3 Use Case Name:

Actors:

Description:

Alternate Path:

Pre-condition:

Use Case no: 4 Use Case Name:

Actors:

Description:

Alternate Path:

Pre-condition:

//html code for the home page, will style and give functionality with css and js//

```
<!DOCTYPE html>
```

```
<html>
```

```
<head>
```

```
  <title>Homepage</title>
```

```
</head>
```

```
<body>
```

```
  <header>
```

```
    <h1>Welcome to Lock In</h1>
```

```
  </header>
```

```
  <nav>
```

```
    <button id="login-button">Login</button>
```

```
    <button id="signup-button">Sign Up</button>
```

```
  </nav>
```

```
  <main>
```

```
    <h2>About Us</h2>
```

```
    <p>Welcome Lock In, the most secure graphical password site available Established in 2023 by a group of students at Georgia State our site looks to provide secure access to sensitive data for companies large and small alike. </p>
```

```
  </main>
```

<footer>

<p>Copyright ©2023 Our Website</p>

</footer>

</body>

</html>