

OFFICE OF LOCAL DEFENSE COMMUNITY COOPERATION

Grantee Guide (6.0)

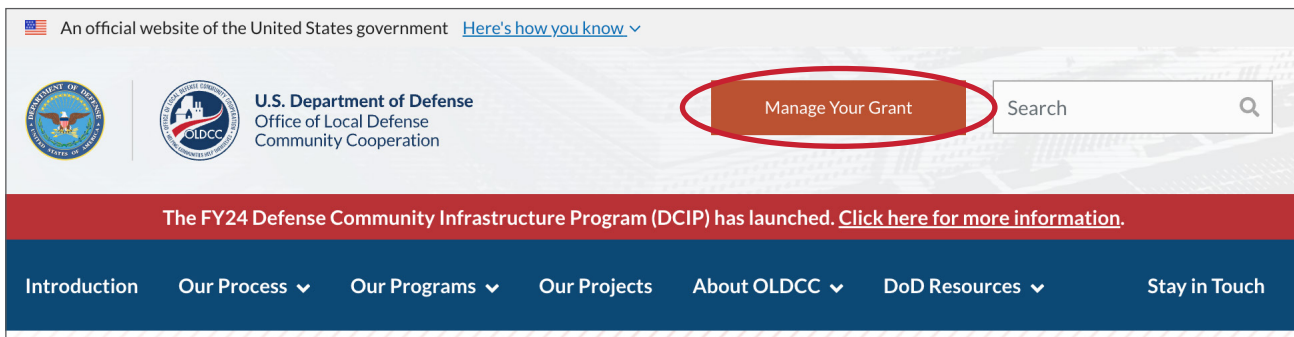
Section A (Login & Password)

OLDCC GRANTS PORTAL

The OLDCC Grants Portal/EADS II requires an email and password to authenticate and allow access to the system. Passwords must be changed before the first log in and every 60 days.

Community users (Authorizing Official, Primary Delegated Authority, Community Contact) must first be added to the system by OLDCC staff before they can access the OLDCC Grants Portal. Once users are successfully in the system, the OLDCC Grants Portal can be accessed one of two ways:

1. Open a new internet browser and enter: https://grants.oldcc.gov/s_Login.jsp
 - a. Chrome and Firefox are the recommended websites, as Internet Explorer blocks some images and icons in the portal.
2. Open via the OLDCC homepage: <https://oldcc.gov>
 - a. Click **Manage Your Grant**.



- b. Click **OLDCC GRANTS PORTAL** when the new page appears.



U.S. Department of Defense
Office of Local Defense
Community Cooperation

COMMUNITY ROLES

Access and edit rights in the OLDCC Grants Portal are defined by the role a user is assigned. Access to the OLDCC Grants Portal is controlled via username and password to ensure only authorized users are performing actions.

Users CANNOT be assigned multiple roles or the workflow will be interrupted. For example, a user assigned the roles of AO and CC will not be able to see the AO's buttons as the system will default to the "lower" permissions (CC).

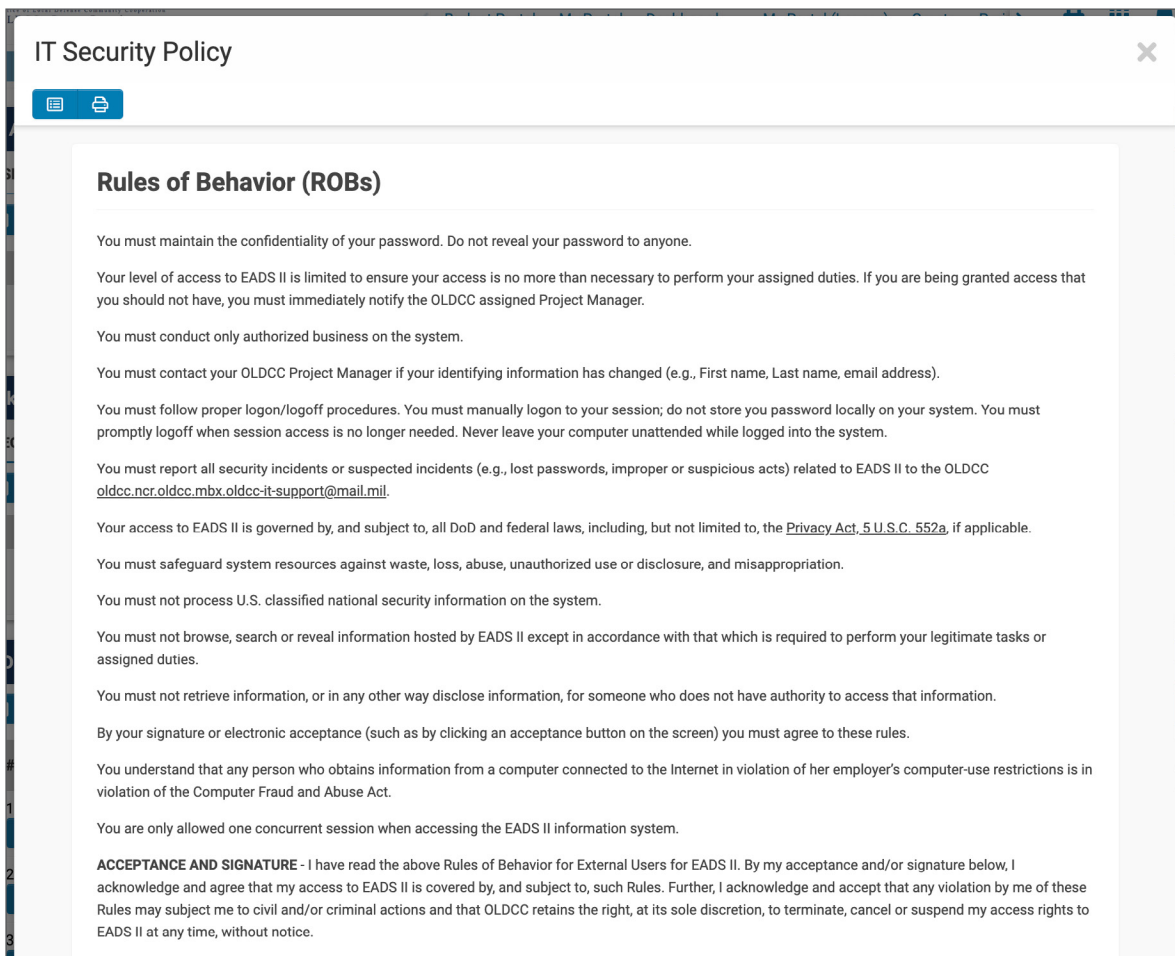
- **Authorizing Official (AO)**
 - The Authorizing Official role is given to the community user who is ultimately responsible for the overall grant.
 - There can be only one AO for a community at any given time.
 - The AO must have the legal authority to enter into financial agreements on behalf of the organization.
 - The AO is the only user with rights to sign the documents to receive any agreed upon funding.
 - The AO has the authority to sign and approve grant applications as well as amendments, the Final Performance Report, and Federal Financial Reports on behalf of the organization.
- **Primary Delegated Authority (PDA)**
 - The PDA is a specific Community Contact who is responsible for completing the application, any requested application revisions, and performing the day-to-day actions (including reports) once a grant has been awarded.
 - The PDA is the counterpart to the PM on the community side.
 - The term "Delegated Authority" means that they are entrusted by the AO to complete actions with respect to OLDCC grants on behalf of the community.
 - An organization can have more than one person with the role of Delegated Authority, but only one "Primary" Delegated Authority at any given time.
- **Community Contact (CC)**
 - The Community Contact role is given to all users on the community side who are authorized by the AO to work on a grant or application.
 - All Community Contacts must be approved by the OLDCC Project Manager and added to the grant before access is granted.

INITIAL LOGIN

The OLDCC Project Manager (PM) assigned to the community organization will add community users as contacts. Once the PM's part is complete, the community user will receive an email to complete the steps below.

Community User Completes Registration

1. Open the email with the temporary password. Click on the **long link** in the email instead of going directly to the portal.
 - a. This link is only good for one use. Once the account is set up following the instructions below, the user should navigate directly to the portal to log in.
2. The OLDCC IT Security Policy (Rules of Behavior) will appear. Acknowledgment and acceptance of these rules is required before use of the system will be granted.



The screenshot shows a window titled "IT Security Policy" with a close button (X) in the top right corner. Below the title bar are icons for a list and a printer. The main content area is titled "Rules of Behavior (ROBs)" and contains the following text:

You must maintain the confidentiality of your password. Do not reveal your password to anyone.

Your level of access to EADS II is limited to ensure your access is no more than necessary to perform your assigned duties. If you are being granted access that you should not have, you must immediately notify the OLDCC assigned Project Manager.

You must conduct only authorized business on the system.

You must contact your OLDCC Project Manager if your identifying information has changed (e.g., First name, Last name, email address).

You must follow proper logon/logoff procedures. You must manually logon to your session; do not store your password locally on your system. You must promptly logoff when session access is no longer needed. Never leave your computer unattended while logged into the system.

You must report all security incidents or suspected incidents (e.g., lost passwords, improper or suspicious acts) related to EADS II to the OLDCC oldcc.ncr.oldcc.mbx.oldcc-it-support@mail.mil.

Your access to EADS II is governed by, and subject to, all DoD and federal laws, including, but not limited to, the [Privacy Act, 5 U.S.C. 552a](#), if applicable.

You must safeguard system resources against waste, loss, abuse, unauthorized use or disclosure, and misappropriation.

You must not process U.S. classified national security information on the system.

You must not browse, search or reveal information hosted by EADS II except in accordance with that which is required to perform your legitimate tasks or assigned duties.

You must not retrieve information, or in any other way disclose information, for someone who does not have authority to access that information.

By your signature or electronic acceptance (such as by clicking an acceptance button on the screen) you must agree to these rules.

You understand that any person who obtains information from a computer connected to the Internet in violation of her employer's computer-use restrictions is in violation of the Computer Fraud and Abuse Act.

You are only allowed one concurrent session when accessing the EADS II information system.

ACCEPTANCE AND SIGNATURE - I have read the above Rules of Behavior for External Users for EADS II. By my acceptance and/or signature below, I acknowledge and agree that my access to EADS II is covered by, and subject to, such Rules. Further, I acknowledge and accept that any violation by me of these Rules may subject me to civil and/or criminal actions and that OLDCC retains the right, at its sole discretion, to terminate, cancel or suspend my access rights to EADS II at any time, without notice.

3. Click **Accept**.

4. If an authentication request appears, complete the request.
 - a. The purpose of authentication is to determine that the first time user entering the system is a real person and not a computer bot.
5. After the initial login is completed, the OLDCC Grants Portal will appear.
 - a. Bookmark the login page for future use.

The screenshot shows the OLDCC Grants Portal interface. At the top, there is a navigation bar with the logo, 'Office of Local Defense Community Cooperation', 'OLDCC: Grants Portal', and links for 'Home', 'https://oldcc.gov/', and 'Payment Forms'. There are also icons for a lock, a bell, and a user profile.

The main content area is divided into two sections:

- Grants Management:** This section has a dark blue header with a '+' icon. Below the header, there are tabs for 'PROPOSED GRANTS (0)', 'AWARDED GRANTS (1)', 'GRANT AGREEMENTS & CLOSEOUTS (1)', 'GRANT REPORTS (15)', 'GRANT AMENDMENTS (3)', 'GRANT DELIVERABLES (4)', and 'KICK OFF MEETINGS'. A search bar is present with a magnifying glass icon and '0 of 0' results. Below the search bar is a table header with columns: '#', 'Project Title', 'Organization', 'Primary Contact', 'Funding Program', and 'Status'. The table content area displays 'No Results Found'.
- Grant Reports:** This section also has a dark blue header with a '+' icon. Below the header, there are tabs for 'UPCOMING REPORTS', 'REPORTS PAST DUE', 'REVISIONS REQUIRED (0)', 'SUBMITTED TO AO (0)', 'UNDER REVIEW (1)', 'FUTURE REPORTS', and 'HISTORIC (11)'. A 'Print' button is visible on the left, and '0 of 0' results are shown on the right. Below the tabs is a table header with columns: 'Grant Name', 'Grant Number', 'Activity Type', 'Date Due', 'Report Period', and 'Status'. The table content area displays 'No Results Found'.

PASSWORD POLICY


When making a new password, keep in mind that the Department of Defense (DoD) mandates that all passwords adhere to the following rules:

- At least one uppercase letter
- At least one lowercase letter
- At least one number
- At least one special character (!@#\$%^&*)
- Have a minimum of 15 characters
- Passwords must be changed every 60 days

Returning Users

Once the community user has been successfully added to the system, they can continue to access the system by following the steps below.

1. Click on the link from the <https://oldcc.gov> homepage or type in the URL (https://grants.oldcc.gov/s_Login.jsp).
2. Read the conditions and click the check box next to **“I have read & consent to terms in IS user agreement.”** The login fields will then appear.

 U.S. DEPARTMENT OF DEFENSE

OLDCC Grants Management System

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and intelligence gathering (IG). This IS includes security measures (e.g., authentication and access controls) to protect USG interest and information.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, inspection, disclosure or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interest and information.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searches on this IS. Privileged communications, or work product, related to personal representation or services by attorneys, agents, or other authorized representatives, are not subject to routine monitoring, inspection, disclosure or use for any USG-authorized purpose. Such communications and work product are private and confidential. See User Agreement for more details.

I have read & consent to terms in IS user agreement.

Login

Email:

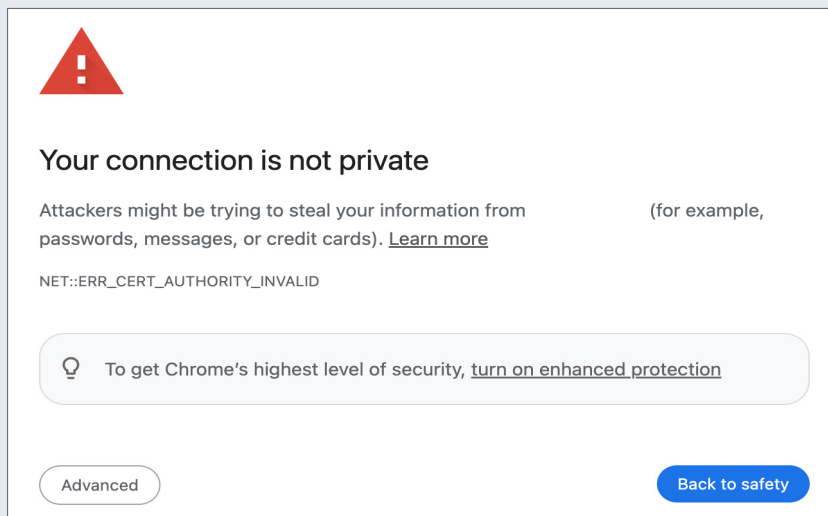
Password:

[Forgot Password?](#)

CERTIFICATES AND ADVANCED SETTINGS:

If the web browser alerts users that the OLDCC Grants Portal may be harmful, follow the instructions below. The OLDCC Grants Portal has a server certificate that was issued by DoD, not a publicly recognized certificate authority, and the site is **not** harmful.

1. Navigate to the OLDCC Grants Portal using the preferred web browser.
2. Most browsers will have a screen similar to the one below. Click on the **Advanced** button.



3. Click **Add Exception** and add "https://grants.oldcc.gov/s_Login.jsp" and/or "https://oldcc.gov" as an accepted website.
4. If this step doesn't solve the problem, applicants and grantees should try the following two options:
 - a. Reach out to their internal IT department for assistance; or
 - b. Check to see if the text under Advanced has a link. If no link appears at all, clear the browser history and reattempt:
 - i. Clear the history then open a new web browser.
 - ii. Navigate to https://grants.oldcc.gov/s_Login.jsp.
 - iii. Click **Advanced**.
 - iv. There should now be a link that says **Proceed to [link] (unsafe)**.
 - v. The link is safe, click to proceed.

PASSWORD HELP

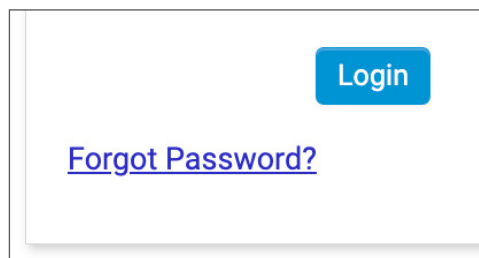
Community users can follow the directions below for passwords that need to be changed or were forgotten.

NOTE:

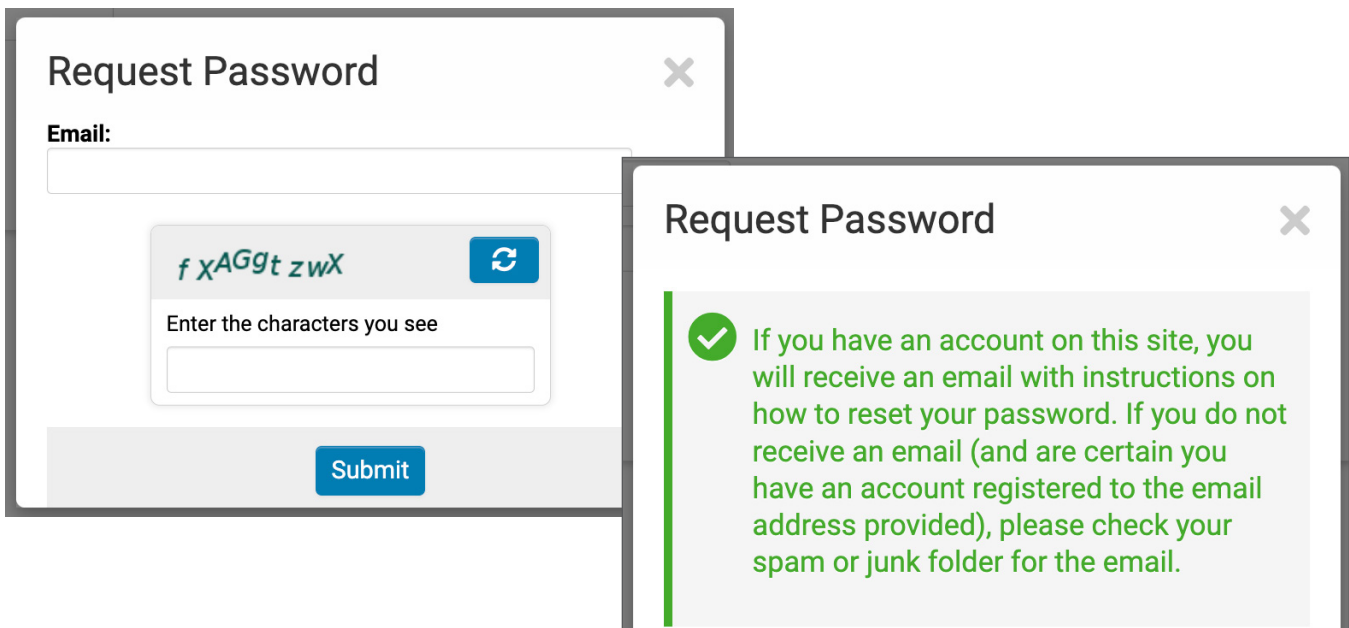
NEVER provide password or account information to another individual. Doing so is a violation of DoD policy and could result in account suspension.

Forgotten Password

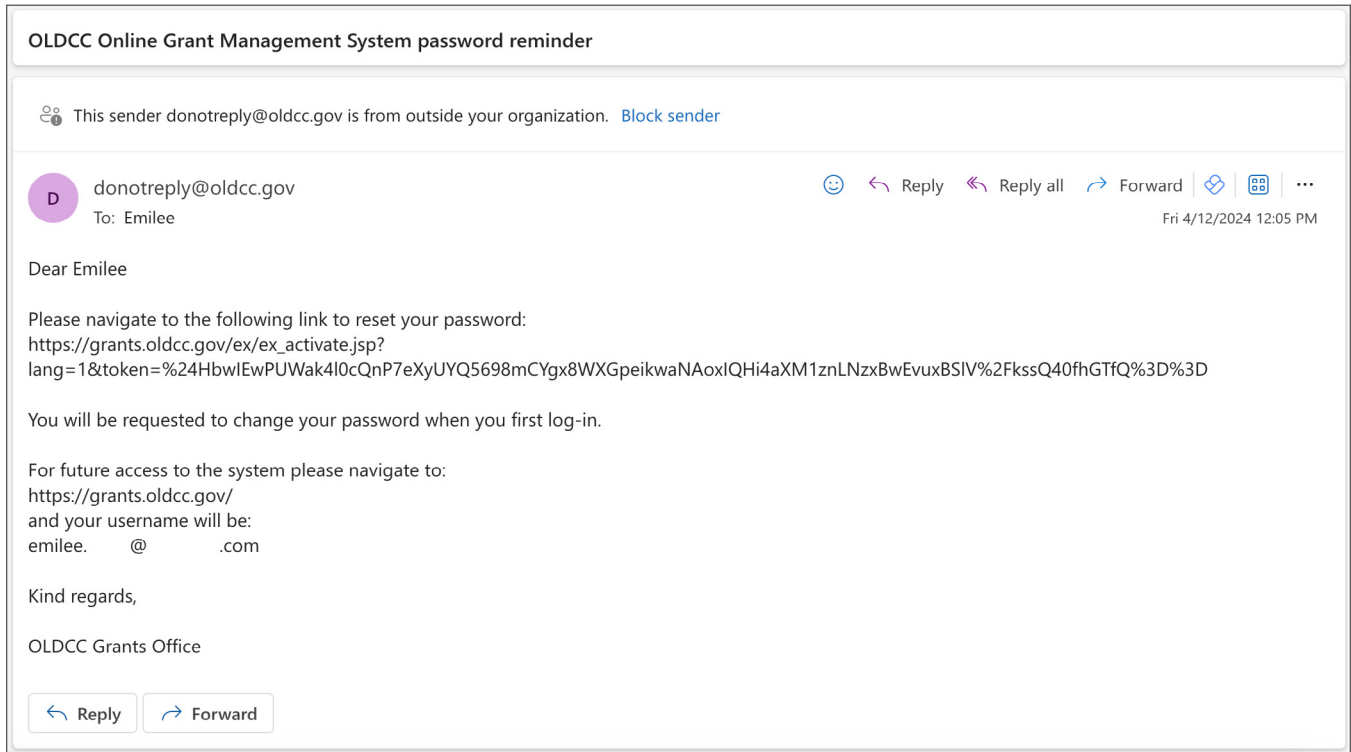
1. Go to the main login screen for the OLDCC Grants Portal and click on the **Forgot Password** link.



2. A pop-up window will appear, requesting the user's email address.
3. Click **Submit**.
 - a. This will send an email with a link to reset the password.

A screenshot of a "Request Password" pop-up window. The window has a title bar with "Request Password" and a close button (X). Inside, there is an "Email:" label followed by an empty text input field. Below the input field is a CAPTCHA box containing the characters "f XAGgt zWx" and a refresh button. Underneath the CAPTCHA is the instruction "Enter the characters you see" and another empty text input field. At the bottom of the window is a blue "Submit" button. A second, smaller "Request Password" window is overlaid on the bottom right, containing a green checkmark icon and the text: "If you have an account on this site, you will receive an email with instructions on how to reset your password. If you do not receive an email (and are certain you have an account registered to the email address provided), please check your spam or junk folder for the email."

4. Click on the long link in the body of the email.
 - a. Copy and paste the address into an internet browser if the link isn't working.



5. Follow the password policy on page A-4 to create a new password.


Password Reset

New Password:

Confirm Password:

Policy: Password must have at least 15 characters

1 of each of the following character sets: - Upper-case - Lower-case - Numbers - Special characters (e.g. ~ ! @ # \$ % ^ & * () _ + = - [] / ? > <)]

4^YFRd3Q²Q 

Enter the characters you see

6. Enter the characters then click **Submit**.

Changing Password

1. Passwords must be changed every 60 days, or when reset by a Project Manager.
2. Enter the email associated with the account.
3. Enter the current password, or the one that was provided when reset.
4. Enter the new password and confirm that it matches.
5. Click **Submit**.
6. At this point, the user should be able to get back into the system.

Change Password

Current Password:

New Password:

Confirm New Password:

Password must have at least 15 characters

1 of each of the following character sets: - Upper-case - Lower-case - Numbers - Special characters (e.g. ~ ! @ # \$ % ^ & * () _ + = - [] / ? > <)

NOTE:

For any of the following errors, reach out to the OLDCC Project Manager or Grants Management Specialist for assistance.

1. Applicant/grantee did not receive a password after clicking reset password link.
2. Applicant/grantee did not receive a password even after #1 was addressed.
3. Applicant/grantee received a password, but still can't log in.
4. The applicant/grantee used a different email than the one OLDCC used to create the account.
5. The applicant/grantee cannot access the portal. (First, verify that certificates are allowed following the steps on page [A-6](#).)
6. The AO cannot see certain buttons.