

# User Roles and Responsibilities

## Do Not Pay Portal Quick Reference Card

### Getting Started

User roles and responsibilities exist in the Do Not Pay (DNP) Portal to ensure that each agency program only has access to their approved data sources and functionalities. Each agency has a hierarchy in the DNP Portal, which is split into Levels and Access Groups. There are various roles found within a hierarchy: the Access Group Administrators (AGAs)—being the Authorizing Official (AO), Primary Local Security Administrator (PLSA), and Local Security Administrator(s) (LSA)— and the non-administrative role of a Portal User.

**An individual can only hold one role within the hierarchy.**

### Access Group

Members of an Access Group have specific authority and visibility to agency data, data sources, and functionalities.

- An Access Group is typically established for each specific agency program, so there can be multiple Access Groups within an agency.
- Individuals **can only** view their data sources approved for their specific Access Group.
- Individuals can see payee, payment, or Payment Automation Manager (PAM) files for their Access Group *and* in any subsequent lower level groups *(that they are approved for)*.
- Individuals can only be enrolled in **one** Access Group within the overall hierarchy.

### Authorizing Official

Each agency hierarchy must have a designated AO which functions as the highest authority over the hierarchy.

- AOs **do not** have access to the DNP Portal.

- AOs are the only authority permitted to make decisions on behalf of the agency's entire hierarchy structure.
- AOs oversee modifications of Access Group abilities; this includes which functionalities, data sources, and individuals are assigned to each Access Group.
- AOs are responsible for informing their Agency Lead and Agency Specialist of any role changes within the Access Group.
  - ◇ *This includes the yearly recertification process.*
- AOs can sign off to approve Access Group Forms, File Association Forms, and User Enrollment Forms.

### Primary Local Security Administrator

There **must** be one PLSA for a hierarchy.

- PLSAs **can only** access the Reports functionality in the DNP Portal.
- PLSAs serve as a backup to the AO by helping with tasks including:
  - ◇ Overseeing modifications of an Access Group's abilities
  - ◇ Informing Agency Lead or Agency Specialist of any role changes within the Access Groups
    - ⇒ *Including during the yearly recertification process*
  - ◇ Signing off to approve Access Group Forms, File Association Forms, and User Enrollment Forms

### Local Security Administrator

The LSA is not a required role, but multiple LSAs may be established throughout the hierarchy.

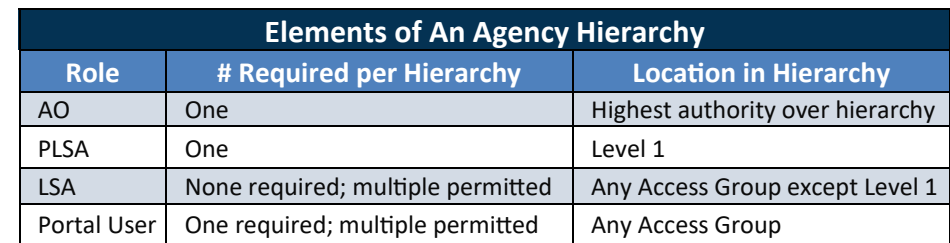
- LSAs **can only** access the Reports functionality in the DNP Portal.
- LSAs oversee similar responsibilities as the AO and PLSA within their own Access Group and the lower levels subsequent to them such as:
  - ◇ Coordinating with the AO and PLSA in managing the Access Group's abilities, users, and roles
    - ⇒ *Including during the yearly recertification process*
  - ◇ Signing off to approve Access Group Forms, File Association Forms, and User Enrollment Forms

### Portal User

The Portal User is the only non-Access Group Administrator role in the hierarchy. There are **no restrictions** on the number of Portal Users an Access Group can have.

- Portal Users are assigned different Levels based on the needs of each Access Group (Level 1 Portal User vs. Non-Level 1).
- Portal Users **can use** the Online Search functionality.
- Portal Users **can view** all Batch Matching, Continuous Monitoring, and Payment Automation Manager (PAM) files associated with their Access Group *(also data files associated with any lower level Access Groups they are approved for)*.
- Non-Level 1 Portal Users are able to adjudicate PAM Payment files within the DNP Portal; however, only Level 1 Portal Users can submit the hierarchy's PAM Payment Adjudication each month.

Below is an example of an agency hierarchy with its respective Access Groups, Levels, and user roles.



## User Capabilities

Below is a chart to outline some of the user capabilities available within each role in the hierarchy. **An individual can only hold one role within the hierarchy.** It is important to remember that users can only access the data sources, functionalities, and reports approved for their specific Access Group. Some may be able to see data files (i.e., payee, payment, PAM) for the subsequent lower level, if approved.

User Capabilities									
Role	Makes decisions on hierarchy structure	Can modify Access Groups' abilities	Notify if roles change	Can sign off to approve forms	Responsible for yearly user Recertification	Upholds confidential nature of data	Has access to Portal functionalities	Has access to reports in Portal	Can adjudicate payments
AO	✓	✓	✓	✓	✓	✓			
PLSA		✓	✓	✓	✓	✓		✓	
LSA		✓	✓	✓	✓	✓		✓	
Portal User						✓	✓	✓	✓

*\*Please note that non-level 1 Portal Users are able to adjudicate PAM Payment files within the DNP Portal; however, only Level 1 Portal Users can submit the hierarchy's PAM Payment Adjudication each month.*

### Important Links

#### FAQs

<https://fiscal.treasury.gov/dnp/faqs.html>

#### What Can I Search?

<https://fiscal.treasury.gov/dnp/search.html>

#### Agency Support

For questions regarding the DNP Portal, contact the Agency Support Center at 855-837-4391, or by email at [donotpay@stls.frb.org](mailto:donotpay@stls.frb.org).

For general inquiries, please contact your Fraud Prevention and Financial Integrity (FPFI) Agency Lead and Agency Specialist, or email [FPFIoutreach@fiscal.treasury.gov](mailto:FPFIoutreach@fiscal.treasury.gov).