Data Protection

A key approach to data protection for Florida PALM includes securing access with user IDs and passwords, assigning permissions, and applying data masking to protected data elements. Protected data elements include confidential information as defined in Florida law. In addition, as Florida PALM evolves, additional protected data elements may be identified that require enhanced data protection measures. When data elements such as these are identified, the Florida PALM team will add these protected data elements to the Project's protected data inventory and apply data masking as appropriate.

Data masking protects confidential information from being viewed by hiding or partially hiding the actual data with characters that conceal the true data on the application pages. The most recognizable implementation of data masking is when a password is hidden after being typed into an input field (i.e. *********).

The Florida PALM system will protect personally identifiable information, as outlined below.

Personally Identifiable Information

Personally Identifiable Information (PII) is any information that can be used to distinguish or trace an individual's identity (e.g., Social Security Number) and any other information that is linked or linkable to an individual (e.g., date of birth) to successfully recognize an individual. Examples of PII include, but are not limited to:

a. Name: first name or last name,
b. Personal identification numbers: Social Security Number, taxpayer ID, bank account number, or credit card number
c. Personal information: street address, email address, personal telephone numbers, or benefits information

The above examples on their own do not constitute protected data as more than one person could share these traits. However, when linked or linkable to one of the above examples, the following could be used to identify a specific person: telephone number, mailing or email address, geographical indicators, employment information, benefits information, financial information.

Sensitive Information

Sensitive Information is defined as information that if lost, compromised, or disclosed could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual or organization. The three main types of sensitive information are personal information, business information, and classified information.

a. Personal information is any data that can be linked to an individual and if released could result in harm to the person. Examples of such information include; social security numbers, passport numbers, biometric information, medical data, and personally identifiable financial information. If such information is stolen it can result in personal information getting into the wrong hands as well as identity theft.
b. Business information relates to any data that would cause damage to a company if accessed by a competitor or the public. This can include financial data, trade secrets, supplier information, customer data as well as other sensitive materials.

c. Classified information relates to any information that a government body restricts due to security concerns. Different levels of sensitivity exist often with labeling such as; restricted, secret, top-secret and confidential. Often over some time, this information is declassified and eventually made public once it's been considered that the risk of harm has passed.

We are mindful that these data protection techniques may impact certain Agency efforts (e.g., Role Mapping activities), as data masking in production may prevent a user from viewing protected data required to perform certain business functions. For example, if a user requires visibility to an entire account number to perform verification functions, their assigned role may impact the ability to execute their job effectively if unable to view the protected data. In such a case, they may require an alternate role. Agencies should consider each users' roles and specific business need to view protected data when performing role mapping activities.

Since Florida PALM will apply this data protection technique, it is important that data not be sent to the Project outside of established data transfer mechanisms for Florida PALM. This ensures that the data is not duplicated or stored in unmanaged locations outside of Florida PALM. Sending data outside of these channels may result in the data not being adequately protected, which could lead to interception by unauthorized individuals. Specifically, for protected data elements, Florida law requires encryption for transmission of this information.

Table 1 identifies the PII and sensitive information that will be protected from full view for all end user roles in Florida PALM, with the following exception as noted in the second column:

Table 1: End User Roles Able to View Protected Data

Florida PALM Protected Data	End User Roles Able to View Protected Data
The following data is masked in Florida PALM based on end user role: • Bank Account Numbers • Personally Identifiable Information (PII), such as names, social security numbers, addresses, etc.	Only DFS end users assigned the following roles will have full access to view protected data: • DFS Bank Reconciliation Processor • DFS Transfer Approver • Book to Bank Reconciliation Processor • DFS Correspondence Processor • DFS Payment Cancellation Processor • DFS Bank Account Maintainer