Data Protection Approach

Overview

The Data Protection Approach describes how Florida PALM manages protected data and identifies end user and agency responsibilities for managing these items outside of Florida PALM. Protected data refers to confidential, exempt, personal, sensitive, or classified information identified in law, rule, or by external parties (e.g., Federal government, other). Florida PALM secures access for protected data with access controls, data masking, data obfuscation, restricted data sharing and data encryption. As additional Florida PALM functionality is implemented, the Florida PALM team will validate whether additional or updated controls are appropriate.

How Florida PALM Protects Data

Multiple controls are used to manage and restrict access for protected data in Florida PALM. These controls are described below.

Access Controls

End users must have appropriate credentials to access Florida PALM data and functionality. Privileges and access are based on end user role assignments. There are a specific roles identified which can access protected data. Agencies are responsible for role assignments and ensuring that appropriate background checks are completed for the end users.

Data Masking

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 PALM application pages. The most recognizable implementation of data masking is when a password is hidden after being typed into an input field (i.e., *********).

Data Obfuscation

Data obfuscation (i.e., changing data) is applied in select non-production environments to prevent inappropriate exposure of protected data.

Restricted Data Sharing

End users cannot share reports or files directly from Florida PALM. Data is only shared in accordance with established data transfer mechanisms for Florida PALM. End users must have the appropriate role to directly access confidential information.

Data Encryption

Interface files use data encryption to protect data in case of interception by unauthorized individuals, by making the content appear scrambled if intercepted.

- **Data Encryption in Transit:** Data will be encrypted in transit leveraging the Federal Information Processing Standard (FIPS) 140-2 compliant with minimum cryptographic algorithm of 256-bit Advanced Encryption Standard (AES). Internet Protocol Security (IPsec) tunnels are used to protect Florida PALM application traffic across an IP network. IPsec tunnels will be established for Secure Virtual Private Network (VPN) tunnels.

- **Data Encryption at Rest:** Application and database level encryption will be used for data encryption at rest. Backup data will be encrypted using AES 256-bit encryption.

Agency Responsibilities

The data protection techniques outlined above may impact certain agency processes and role assignments. For example, if an end user requires visibility to an entire bank account number to perform verification functions, the end user will need the appropriate role assignment to execute their job effectively. Agencies should consider the duties of each user and whether access to confidential data is required when assigning roles. Agencies may change role assignments to accommodate employee duties. Agencies should refer to the Role Assignment Approach for more information.

In instances where end users have a business need to use protected data outside of Florida PALM, the end user must protect the information within agency internal control mechanisms. For example, if the end user prints a report containing exposed protected information, the hardcopy report should be stored in a locked or secure drawer or office. If the end user shares information electronically (using e-mails or other file sharing mechanisms), appropriate agency protocols should be followed for protected data.