PIDS Security Documentation

Web Application Security

Physical Security

- All physical security for the PIDS web application is handled by the Microsoft corporation since the web application is hosted in Microsoft Azure.
- More information can be found here: https://learn.microsoft.com/en-us/azure/security/fundamentals/infrastructure

Digital Security

- Configuration of the PIDS web application servers is restricted to specific Microsoft accounts that are authorized on a person-by-person basis by the Center for Human Services Research at UAlbany. The security of those accounts is covered by UAlbany policies and procedures as well as Center for Human Services Research policies and procedures.
- The web application requires connections using HTTPS protocol. This protocol helps ensure security through encryption of the communication between the user's browser and the web application server.
    - The web application is configured to use a Microsoft-issued SSL certificate.
- Files that are uploaded to PIDS are stored in an Azure storage account, and access to configure the account is restricted to specific Microsoft accounts that are authorized on a person-by-person basis by the Center for Human Services Research at UAlbany. The security of those accounts is covered by UAlbany policies and procedures as well as Center for Human Services Research policies and procedures.

Database Security

Physical Security

- All physical security for PIDS databases is handled by the Microsoft corporation since the databases are hosted in Microsoft Azure.
- More information can be found here: https://learn.microsoft.com/en-us/azure/security/fundamentals/infrastructure

Digital Security

- Configuration of the PIDS database servers is restricted to specific Microsoft accounts that are authorized on a person-by-person basis by the Center for Human Services Research at UAlbany. The security of those accounts is covered by UAlbany policies and procedures as well as Center for Human Services Research policies and procedures.
- Data is protected by Azure's transparent data encryption feature. More details can be found here: https://learn.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview?view=azuresql&tabs=azure-portal
- Comprehensive backups of the databases are maintained through Microsoft Azure's backup features. More details can be found here: https://learn.microsoft.com/en-us/azure/azure-sql/database/automated-backups-overview?view=azuresql

- Measures are in place to automatically record actions that are taken on the data in the databases.

User Account Security

- User accounts are managed by a state-level administrator. This includes creation of new accounts, setting permissions for accounts, and deactivation of accounts.
- Users are required to confirm their accounts before they can log in for the first time. This is accomplished through an automated process that starts when the state administrator creates their account.
- Users are required to agree to state-specific policy document that outlines how they can use the PIDS system and the data contained within PIDS. If the user does not agree to follow the policies in the document, they will be unable to utilize the system.
- Users have the option to use two-factor authentication to add an additional layer of security to their accounts. Two-factor authentication codes can be received using the below methods:
  - SMS message. This requires that the user has added a confirmed mobile phone number to their account.
  - Email.