Application Security Protocols

Overview

R3Dashboard security protocols are managed via developer and staff policies and procedures related to the application itself, the data therein, and the files and data used to compile the application.

Application Infrastructure

Hosting

The application is run from a PaaS (Platform as a Service) hosting environment at Heroku. As a world-class PaaS provider, Heroku (parent company Salesforce.com) has a strong commitment to the security of its service offerings. Details can be found at https://www.heroku.com/policy/security.

ClearDB

The database underlying R3Dashboard is hosted via a service from ClearDB. ClearDB instances leverage encryption everywhere: data at rest is encrypted, backups are both compressed as well as encrypted, and network encryption is available using MySQL SSL support. ClearDB also employs strict operational controls on data access to prevent unauthorized personnel from accessing application data without explicit permission.

TLS Protocols

The application is currently served using TLS cryptographic protocol version 1.3.

User Accounts

Sensitive Data

User accounts include the following personally identifiable information:

- First and last name
- Email address
- Mobile phone number *(if two-factor authentication via text message is enabled by the user)*

Collection of other personally identifiable data for user accounts is not expected at this time.

User accounts may be associated internally with a sponsoring organization.

Passwords

Passwords for user accounts are encrypted before storing, plaintext passwords are not stored or accessible. Application log files are configured to exclude passwords and other sensitive information.

Password rules require at least 12 characters.

Password resets are managed via an email sent to the account email address and must be completed within 6 hours.

Two-Factor Authentication

Two-Factor Authentication via email or text message will be implemented prior to go-live. 2FA will be encouraged, but not mandatory.

Account Settings

User accounts are locked after 5 failed login attempts. Accounts can only be unlocked via an email sent to the account email address.

User account email changes require authentication via an email sent to the (original) account email address.

User notifications are sent upon user account email and password changes.

Sessions

Sessions are logged out after 60 minutes of inactivity.

Developer Access

Application

Developers who are actively developing and/or supporting the project are granted full access to the application under the Developer role. Developer accounts use strong passwords and two-factor authentication (when implemented).

Services

Developer access to the R3Dashboard hosting and infrastructure services is granted on an as-needed basis only.

Service accounts use strong passwords and two-factor authentication, where available.

Service account passwords are rotated on a regular basis.

Service accounts are not shared.

Data/Data File Transfer

Data/data files are transferred to R3Dashboard via secure, encrypted channels. Transferred data/data files are not accessible publicly via the application or storage platforms.

Data provided to R3Dashboard does not include personally identifiable information beyond the following minimum required data:

- CUSTOMER_ID *(required for accurate retention/recruit categorization)*
- DOB or BIRTHYEAR or AGE *(required for accurate demographics reporting)*
- GENDER *(required for accurate demographics reporting)*
- RESIDENCY *(required for accurate demographics reporting)*
- SALES_ID *(required for duplicate data prevention)*

Data Retention

Data files provided to R3Dashboard are maintained for a period specified by the state/vendor (7 – 30 days recommended), to ensure the data is loaded accurately, and then removed from all storage platforms.

Data loaded from these files is maintained in the database until the end of the sixth year after the transaction year for which the data is provided, so that retention/recruit statistics can be compiled. It is then removed from the database.

Summary data compiled from the detailed data provided by states is maintained in the database indefinitely for ongoing reporting purposes.