PLAYER MAP X-RAY

Player Map X-Ray for Salesforce® passed the rigorous Salesforce® security review

- PMX accesses Salesforce® data (user, account, opportunity and contact objects) via the Force.com® API through a 256-bit encrypted channel (SSL Version 3 over HTTPS).
- PMX users are only able to access Salesforce® accounts, opportunities and contacts they have rights to within Salesforce® for creation of Player Maps in PMX.
- When PMX accesses Salesforce® data via the Force.com® API, all Salesforce® access controls that apply to the Salesforce® user accessing PMX also apply to data access.
- PMX is accessed via SSL, so all data sent to and from PMX via the Force.com® API or with the user's interaction with the application is encrypted.
- Player Map data that PMX stores includes contact data (i.e. name, title, location, phone & e-mail), Salesforce® account or opportunity ID, and the Salesforce® username.
- PMX does not use or share any data that is captured by the app except to generate Player Maps, and the user controls who sees their Player Maps via folder sharing.
- Clients can immediately delete individual PMX account through Org Admin, and all data for suspended users is permanently purged after 30 days from suspension.

If questions, ping us at pmx@playermap.com or 1.414.921.2550