INFIMA

Protecting your Information

Security is built into all of our services to protect customer information

All INFIMA products are designed and built with security in mind. We limit the amount of data collected to only that required to successfully deliver our services. In most cases, the customer data we store is limited to the following:

- Company name
- Employee first and last name
- Email address
- Phishing and Training results

We work hard to limit the data we collect from you and ensure your data is protected from unauthorized access, alteration, disclosure or destruction including:

- Multi-layered security for your production data
- Multiple access stages for viewing internal client data
- Encrypting identifiable data to maintain privacy while in transit
- Support for the latest OAuth 2.0 authentication protocols
- Regular review of our design practices, infrastructure requirements and employee processes to prevent unauthorized access to our systems
- Strict internal employee access controls limit data access only to those required. Each employee with these privileges is subject to strict contractual confidentiality obligations and may be terminated or prosecuted if they fail to meet these obligations.

INFIMA

Protecting your Information

Utilizing modern APIs to increase security and improve ease of use

At INFIMA we take advantage of new technologies offered by our partners to improve our client experience and eliminate potential attack vectors.

Microsoft Graph API

We are an approved Microsoft Partner and Publisher, validated by the blue badges on all Microsoft OAuth Consent Pages. This requires successful completion of Microsoft's Partner Network vetting process.
We utilize Microsoft's Graph API for the following features:

- User Authentication
- User Sync
- Group Sync
- Secure Email Delivery/Assured Delivery

Google Directory API

Our Authentication and Sync applications were reviewed and verified by Google under their Google Cloud Platform Verification process.
We utilize Google's Directory API for the following features:

- User Authentication
- User Sync

Secure Partner Interface Approach

Our partner interface architecture follows the recommendations outlined in Microsoft's Graph Best Practice Document. This includes using least privilege consent based on scenario, a multi-tenant

architecture which isolates client data, and receiving minimal responses (minimizing what client data is sent over the wire). All Microsoft Graph API and Google Directory API communication is over encrypted channels, using modern TLS cyphers.

Our development and operational support processes adhere to Google's Securing API Keys Document. API keys are never stored in source code nor are they included in our application source repository. API keys are stored encrypted by AES 256-bit keys utilizing Amazon Web Services' Key Management Service.