Immigo Security

You trust us to keep your valuable and sensitive data safe: to keep it confidential, backed up, secure from attack, but available to the right people when it is needed.

We take that trust very seriously. That's why we have implemented the following systems and measures.

We Are ISO 27001 Certified

We have achieved certification to the internationally recognised ISO 27001 Information Security standard, demonstrating our firm commitment to client data security and confidentiality.

To become certified, a company must implement over 100 mandated controls and undergo a formal audit that confirms that they are compliant with the requirements set forth by the standard.

Certified organisations are committed to continuous improvement and are assessed annually to ensure progress is being maintained through an internal audit program.

Information Security Management System and Policy Objectives

Peregrine maintains an Information Security Management System and Information Security Policy, the objectives of which are to protect all in-house and client data from unauthorised access, to meet all legislative, regulatory, contractual and business continuity requirements and to preserve:

- **Confidentiality** - Access to data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

Data Ownership

You own all right, title and interest in and to all of your data, and Peregrine will return any and all of your data to you on request.

Security of Core Technologies

- We host our software on up-to-date patched GNU/Linux systems. Those systems are configured to only ever expose client data to authenticated users over channels encrypted with OpenSSL.
- Immigo servers are configured with the minimal possible attack surface-- the database, file-system, etc. are not accessible via any protocol except SSH (used for backups and administration) and HTTPS (for end-users).

Hosting Security

Sensitive client information is stored in the Immigo databases on secure remote virtual servers located within outsourced data centres managed by multiple hosting providers. These data centres maintain strict security protocols including:

- 24/7/365 external and internal CCTV with keyholding and police response
- Access control system with all doors having individual shoot bolts; individually discriminated and controlled access for different areas
- All racks and contained aisles are locked
- VESDA system and double-knock fire alarms with FM200 gas suppression
- Category 3 intruder alarm with automatic keyholding and police response; alarms generated to on call engineers

The choice of hosting providers and agreements with those providers are reviewed regularly to ensure that they meet the Information Security Objectives.

Backup and Archiving

Databases are backed up every two hours onto another secure virtual server in a different data centre in a different location, and every day onto a secure office hard drive, using rsync over ssh.

Continuity

In the event of main server failure, we will inform clients, suppliers and staff and will provide an alternative URL to access the databases on a backup server.

Access and Passwords

- All access to sensitive client data and documents is controlled within Immigo, by means of secure, password-protected user accounts.
- Immigo does not allow access over HTTP, only encrypted HTTPS. HTTPS

has been configured to only use the most secure ciphers available. SSLv3 is disabled meaning, for example, that attacks like the recently-publicised POODLE attack will not work.

- In addition, we record all accesses to Immigo in system logs.
- You can grant limited access to data held in Immigo to your clients, by creating "**user accounts**" for them. User accounts are configured so that your clients access only what they need to see. You have complete control over their level of access.
- Passwords are not stored anywhere on the system. Instead, we store cryptographic hashes, which cannot be used to access anyone's account or any sensitive data.
- It is only possible for users to change their passwords over encrypted connections.

Cryptography

Internally Immigo uses AES(Advanced Encryption Standard)128 for encryption of urls, passwords, encoded form data (when registering new accounts), and other purposes.

Data is encrypted "in transit" (i.e. on the way in to and out of Immigo) and, on client request, can also be encrypted "at rest", using Rijndael-256.

URL Access

All access to Immigo through Apache is via the specific Django applications that we run to provide the service. There is therefore no possibility of anyone gaining access to any other stored documents or data on the server except via the Immigo user-interface. All Immigo view functions check the access level to the object before going any further.

Protection from Attacks

We run regular vulnerability and penetration scans to ensure that our software is secure from malicious attacks. Here's a list of threats and the specific measures we take to protect against them:

Injection and XSS

- Immigo is protected from injection of malicious data by validating lengths, types and content of all form data before it is stored in the database or returned in any way.

- Data storage is always via an ORM so there is never anything resembling direct evaluation of strings returned from the user, preventing any possibility of an injection attack.
- In addition, rendered content all goes through a template engine whose default behaviour is to escape all tags, so that even if injected code did get in, there is no way it would get back out again in an executable form, thus an XSS attack would not be possible.

Authentication and Session Management

- All Immigo functions require the user to be authenticated.
- Authentication is tracked using a secure HTTPOnly cookie that contains no information except a cryptographic nonce that is recognized by the server, which is where the actual session-specific information is stored and remains. HTTPOnly cookies are secure cookies, which means that they are only ever sent over encrypted connections; i.e. sessions cannot be stolen by attackers using packet-sniffers.

Insecure Direct Object Reference

- All database objects are identified in URLs only by encrypted strings (for example /immigo/case/id-7400s11qmoob5q7TmOozvDT1Uw==/). The encrypted object ids make it impossible to guess urls to other objects in the database. They also prevent leakage of any information about the order in which objects may have been inserted or by whom.
- Even if an attacker had obtained a url to an object he/she didn't have access to by some other means, he/she wouldn't be able to access the object anyway: as soon as any attempt is made to read or write an object, after decrypting the id, the system checks whether the logged-in user has access to read or write that object. If not, it returns an error and goes no further.

Cross Site Request Forgery

All forms, including AJAX requests, use CSRF tokens which are validated on the server.