KMD - Organised

Security Statement

Revision 2

Date October 2016

The KMD Organised wealth and document portal employs advanced security features and protocols keeping data safe, private and secure 24/7, 365 days of the year. Password protection, data encryption and secure server hosting facility are key components of a safe and user friendly wealth service.

KMD Organised
Stansted Office
The Barn Office, 1 Pond Lane, Bentfield Road,
Stansted, Essex, CM24 8JG

Supported by

Contents

Security Statement

This statement answers the key questions related to data security for the KMD Organised system.

No Financial Transactions

Your money cannot be moved, withdrawn or accessed on the KMD system, this is not an online banking or shopping website.

Data and encryption

There are 2 types of data stored:

- Scanned documents
- Other data about the clients and their documents. Some of this is meta data about the documents but much of it is data about the client and their vaults.

Data in Place – Scanned documents

The scanned documents are stored on the server in a folder that is not exposed to the internet and are only accessible to an authenticated user via the secure Organised web application.

Data in place – Other data

All data other than the scanned documents are stored in a Microsoft SQL server database. Any identifiable client fields are stored as an encrypted binary data blob so that if an unauthorized person got access to the data then they would not be able to use it unless they have the encryption key. This key is only available to the application.

Data in Transit

Offsite backups are transmitted across the internet as a password protected zip of a significantly encrypted database. The encrypted database has no user recognisable data that is not encrypted.

Application and password protection

The system comprises of:

- A web application (VB.NET)
- A desktop app to upload documents. (VB.NET)

Web Application Security

SSL/ TLS Encryption. All requests to the system will be encrypted between the server and the browser

User Authentication: User data on our database is logically segregated by account-based access rules. User accounts have unique usernames and passwords that must be entered each time a user logs on. Sorted issues a session cookie only to record encrypted authentication information for the duration of a specific session. The session cookie does not include the password of the user.

User Passwords: User application passwords have minimum complexity requirements. Passwords are individually salted and hashed.

2 Factor Authentication: Users may opt to have 2 factor authentication. All system administrators will have 2 factor authentication.

Document Upload Tool

The document upload tool accesses the system via an API adhering to the same security principles of the web application.

Hosting

Physical Security

Our hosted server facility is ISO certified where both physical and virtual security is taken very seriously. The data centres have security teams on site 24x7 and are closely monitored using both internal and external CCTV. Data centre access is restricted to a very select number of named staff who are required to have appropriate security clearance and secure fobs to gain access.

Cyber Security

All data is safeguarded behind a multi-layered firewall, backed up regularly and stored offsite.

Power Security and resilience

Each server rack has two independent power feeds, fed from two diverse connections to the national grid. Should one or both of these feeds fail, 4 x 300kVA Riello UPS (N+1) battery backup systems cover immediate power requirements. If mains power is not restored within ten seconds, 3 x N+1 diesel powered generators start providing full continuous power to the data centre.