FileFinder SaaS – Security Information

1. FileFinder Encryption and authentication

a) FileFinder for Desktop (Rich Client)

FileFinder for Desktop is a client/server application that communicates with an SSL certificate over **HTTPS** and transfers data via small data packets.

The FileFinder for Desktop service layer is hosted within Azure App Services and therefore comes with configuration and security built in.

b) FileFinder Desktop, FileFinder Browser & FileFinder Mobile

FileFinder uses a 2048-bit SSL certificate and 256-bit encryption in transit.

c) Data Encryption

SQL Azure TDE (Transparent Data Encryption) ensures all customer databases, backups, and logs are encrypted at rest. Data outside of SQL Azure is stored on encrypted Azure storage accounts (e.g. documents).

d) Forms User authentication

Access is granted to FileFinder by a User ID and Password. The system-wide password complexity requirements, account lockout, forced password resets and password history options are all configurable.

FileFinder has several user security levels that can be assigned to users according to their requirements and the requirements of the company. These allow the user (if access is given by the system administrator) different levels of access as described below:

e) Role Based Security

Organizational Units, Roles and Users are interlinked and are concerned with access to the software. Organizational Units (OUs) are used to map out the structure of your company. In a simple company structure, you would have one OU in which all users can see and manipulate all information. In more complex company structures such as networks OUs can be used to segregate the data so that records created by users in one OU are not available to users in another.

Users, roles, and permissions can all be configured to meet the security requirements of your organisation.

Users are granted one or more roles that define their permissions within the software.

For each entity in FileFinder a User can be granted the following permissions:

- Create – Create new Entity
- Read – Read Only Access
- Update – Update existing Entity
- Delete – Delete Entity

Permissions – A role is a collection of permissions. The permissions available are Create, Read, Update or Delete these can be applied to different entities in the database like People, Companies, Assignments and Reports. You can also restrict exporting and printing.

Levels – Permissions can be given a level. For example you may be able to Update records created in your own Organizational Unit but not those created in other Organizational Unit.

g) **MFA – Multi-Factor Authentication**

This allows users to authenticate logins using a secondary method to authorise access, via an app such as the Microsoft and Google Authenticators.

We use Time-based One-Time Passcodes (TOTP) for MFA.

TOTP-based two-factor authentication involves generating a temporary, unique passcode that is valid for 60 seconds. After generating a six-digit passcode, a user must enter it along with their normal user ID and password to authenticate.

Configuration of 3rd party MFA applications is simple and quick by FileFinder presenting the user with a QR to scan and automatically configures the device.

Configuration options can be applied such as account lockout if a series of invalid login attempts.

3. Cloud security

Our cloud services are delivered using Microsoft Azure

a) Facility security

FileFinder's cloud partner is Microsoft Azure. Azure meets numerous recognised standards such as ISO 27001/27002.

Including:

ISO 27001	https://www.microsoft.com/en-us/TrustCenter/Compliance/ISO-IEC-27001
SOC	https://www.microsoft.com/en-us/trustcenter/compliance/soc
General Compliance	https://azure.microsoft.com/en-gb/overview/trusted-cloud/

b) Penetration Testing

Ikiru People conducts regular penetration testing. Subject to prior Ikiru People and Microsoft Azure notification and approval, we may also allow clients to conduct their own Penetration testing – this cannot be conducted without written approval from a Director of Ikiru People.

c) Configuration Management and version control

Ikiru People uses Azure DevOps to configure, deploy and maintain versioning of the relevant FileFinder applications.

Scheduled maintenance updates are done out of scheduled business hours for the Azure region in use and we aim to provide 7 days' notice in advance. Systems will typically be offline during this period.

d) Network Security

The network is configured to deny access by default other than for required ports. No data is held on public facing servers.

Shared UIDs and passwords are not used. All employees connecting to the Azure environment must do so using a specified individual account. This is limited to the Infrastructure and Implementation teams.

All passwords are stored in a secure system.

Connection to the Cloud Network can only be made via specified IP ranges to specified ranges.

We use Azure Log Analytics to collate and store server, application and other logs. This system collates all information centrally from servers and the information is piped into this system so that it is not held solely on each server which we can report against. We have a monitoring system in place which emails specified groups (all emailed groups contain at least one director) with alerts, as well as monitoring dashboards for visual review. The alerts go to relevant teams in Europe, the USA and Australia to give global coverage.

We aim to notify clients within one hour of a confirmed system outage or other significant issue such as a network breach.

4. Backup and Disaster Recovery

a) Backup

FileFinder SaaS uses the Standard tier of SQL Azure. This provides automatic geo-redundant full, differential, and transactional backups. This means that FileFinder SaaS databases can be restored to the transactional log period, which according to Microsoft is approximately 5 to 10 minutes. Backups are retained for 35 days.

Backup data is stored in geo-redundant storage blobs that are replicated to a paired Azure region.

b) Disaster Recovery

SQL Azure automated backups ensure that the backup data (which is taken every 5-10 minutes) is geographically redundant. In the event of a failure in the primary region, data will be restored within the corresponding paired region and our Azure DevOps release pipelines will deploy a new platform via code.

5. Ikiru People Staff and compliance enforcement

a) Staff onboarding

All staff are reference checked prior to commencing with Ikiru People and must present a copy of their passports upon commencement of their employment, as well as national security numbers. Any members of staff who may come into contract with customer data in the line of their duties undergo additional background checks.

b) Staff leaving

There is a defined procedure for staff departing the company. This sets out amongst other things the removal of physical access to premises, the withdrawal of networking accounts and the removal of any company related equipment.

c) Confidentiality agreements

All staff sign a confidentiality agreement upon commencement of employment with Ikiru People.

d) Ongoing training and meetings

Regular meetings occur across all departments including development, project management, cloud delivery and deployment, network and security, support and account management to ensure compliance and on-going training.

Monthly cyber and data security training is also undertaken by all group staff along with regular simulated threat vectors to ensure training, as well as appropriate procedural, understanding.

e) Risk Assessment

There is a formal risk register which all departments provide input into which is reviewed at board level as well as at management level. It is a permanent item on the board agenda.