Security Guide

CONTENTS

INTRODUCTION

FinCalc is an innovative **Financial Planning Suite** that ensures advisers are equipped with user friendly tools to help them provide clients with fully comprehensive advice. FinCalc incorporates tools such as **Transvas with TVC**; widely used throughout the pensions industry as a means of accurately assessing and analysing Safeguarded pension benefits and **Cashflow Modeller**; our comprehensive approach to cashflow modelling providing the tools to accurately and concisely illustrate the impact of future planning options for even the most complex of situations.

FinCalc is powered by O&M Pension Solutions who have been heavily involved in providing software solutions for the financial services industry for over two decades.

To protect unauthorised access and to protect the data held on it, we have included a comprehensive range of security settings, several of which can, if required, be amended within FinCalc to set up defaults to suit your business requirements.

FinCalc Support Team

If you have any queries related to this guide or encounter any problems using FinCalc, please do not hesitate to contact us as follows:

Email: support@fincalc.co.uk

Tel: 01206 803210

INFRASTRUCTURE SECURITY

We use a secure UK based Microsoft Azure SQL Database System on which to store your data, which is encrypted at rest and in transit. To help organizations comply with national, regional, and industry-specific requirements governing the collection and use of individuals' data, Microsoft Azure & Azure Storage offer the most comprehensive set of certifications and attestations of any cloud service provider. For more information on this please see our **"Security FAQ's''** document.

Our application has undergone a rigorous penetration testing process. Our latest attestation letter is available on our due diligence page. Penetration Tests will be undertaken annually, or prior to any major releases to ensure compliance with our accreditation.

Should you require more detailed information regarding the levels of security we have in place please see our **"Company Policies"** document.

There is an option to have an Isolated Managed Environment, whereby separate instances of the Azure SQL Database, Azure storage for reports and Azure web application are set up dedicated to your Company. This would incur a separate additional cost. Please see the factsheet on our website for more information.

SECURITY SETTINGS SCREEN

System security settings are split into two parts: A: **Company Level** B: **Individual User Level**.

The following are the settings that need to be reviewed and set on a Company Level which will affect all Individual Users of the system. These settings can only be amended by authorised Users via the Security Settings screen. (If a setting is not amended, then the system default will apply).

Password/Login Settings

Passwords are held on the system in an encrypted format (specifically one way hashed using the latest encryption algorithms). Requirements regarding the level of complexity required for a user's password/login are set here.

These include:

- Password expiry time (**system default is 90 days**).
- Minimum password length (**system default is 8 characters**).
- Whether specified characters are required to be included in the password, i.e. upper case, lower case, symbol, number (**system default is that upper case, lower case, and a number are required**).
- Whether a password can be reused again – i.e. A user will not be able to choose the same password as one previously used (**system default is User cannot choose the last password used**).
- Whether any words should not be allowed to be used as passwords. For example, password, welcome, password1234 etc (**system default 'password' is a backlisted word**).
- The number of times a user can make an unsuccessful attempt to login (**system default is five attempts).**
- How long a new password link would be valid for (**system default is 48 hours**).

IP Whitelist

If the Company wishes to limit access to the system from a set location, an IP address list can be set (a **whitelist**). This will lockdown the system to that given list of IP addresses. If no IP addresses are listed, access from any location is permitted (this is the default setting).

If access is limited by the whitelist, users can still access the system from outside of the whitelist if they have the appropriate "Mobile User" security setting under their user profile.

2-Step Verification

For an additional level of security, you can choose to have 2-Step Verification (2-SV) switched on. The specific 2-SV requirements can all be set. To log on to the system a password and a PIN would be required. First, you must pass the password login before you see the 2-SV login screen. The settings are as follows:

- Whether 2-SV is enabled. Switch to Yes to turn on 2-SV for all Users (**system default is No**).
- The length of the PIN. This can be 4, 6 or 8 digits (**system default is 6 digits**).
- How long a new PIN would be valid for (**system default is an hour**).

- How the PIN is delivered to the User. The PIN can be delivered to the User by mobile phone text message, email or by mobile with email backup (**system default is by mobile with email backup**).
- Whether a new PIN is required every time the User logs into the system or, whether the PIN entry is only required once and will not be required again until the PIN expires (**system default is every login**).
- If a new PIN is not required for every login attempt, how often a new PIN is required for each User (**system default is every 7 days**). Please note that PINs are reset at midnight GMT.

Note that if the incorrect PIN is input five times, the User's account will become locked for security purposes (this setting cannot be changed). You will need to contact FinCalc Support to unlock the account.

Client and Record Access

Other system settings to be applied are as follows:

- Whether "All Users see all clients" or "Managed User access to clients"" is selected (**system default is "All Users see all clients"**). Please note, this feature is only available for Enterprise users of the software. (See **Section 7)**.
- The maximum inactive time before a locked record is accessible by another User (**system default is 300 minutes**).
- The maximum time the system can be **"Idle"** before the User is automatically logged out (**system default is 20 minutes**). This must be set to a minimum value of 2 minutes.

To amend any of the settings above, you would simply select the "Security Settings" from the User dropdown menu, edit the required setting and then select "**Save**" at the bottom of the page. All amended settings would apply to all Users when they next log in to the system.

MANAGE USERS' SETTINGS

Manage user settings consist of two elements, Manage User Profiles and Manage Users. Manage User Profiles relates to the access each user profile has throughout the system, these profiles are then allocated to each User within the Manage Users section.

Manage User Profiles Screen

Each User will have a User '**Profile**' assigned to them.

Various levels of User Profiles are available; however you also have the ability to create your own. The system is pre-programmed with Profiles for the following levels of access: "**Power User**", "**User**", **"Transvas User", "Cashflow User"** and **"IT Admin**".

The system is set to have a Power User by default, whom has access to all security options, including the 'Security Settings Screen'. The Power User will, by default, maintain overall control of the system.

The default User, Transvas User, and Cashflow User profiles have more limited security access as default. Users can view all scheme data on the system, Transvas User can only view Transvas data, Cashflow User can only view Cashflow data.

If required, an IT Admin user can also be granted access to certain security settings only, with no access to any client or scheme data. Power Users, Users, Transvas Users, and Cashflow Users would require a chargeable licence. IT Admin Users do not.

For Users that have access, the Manage User Profiles Screen shows a list of available user profile types, with the option to Add a Security Profile and Copy Security Profile.

- **Profile Name** – this needs to be something clear and meaningful to your new Security Profile
- **Settings** – where you can select whether the user can amend security settings, company settings, manage user profiles, manage users and whether they can be a mobile user.
- **Clients** – where you can select whether the user can view all clients, view own and shared clients, edit all clients, edit own and shared clients, create new clients, delete all clients, delete own clients, bulk change adviser (ownership) of clients, share all clients and share own clients. Please note the share options will only be applicable to Enterprise users of the software.
- **Transvas** – whether this user has access to the Transvas with TVC tool. Please note this will only be applicable if you subscribe to the Transvas with TVC tool.
- **Cashflow –** whether this user has access to the Cashflow Modeller tool. Please note this will only be applicable if you subscribe to the Cashflow Modeller tool.
- **Retirement Modeller** – whether this user has access to the Retirement Modeller tool. Please note this will only be applicable if you subscribe to the Full FinCalc Suite or the Cashflow Modeller tool.

- **Calculators** – whether this user has access to the Calculators. Please note this will only be applicable if you subscribe to the Full FinCalc Suite or the Cashflow Modeller tool.

Profiles are allocated to Users under the “Manage Users Screen“.

Manage Users Screen

For Users that have access, the Manage Users Screen shows a list of active Users for the company with the following details: Name, Email address, Mobile Phone number, User Profile (assigned to them)and Team (assigned to them).

Next to each User’s Profile you will see a set of icons as follows:

✏

Note: For those Users that are assigned to an ‘IT Admin’ Profile, you cannot change their User Profile as these Users do not hold a “chargeable” licence. In this circumstance, if you wish to change the User Profile, this has to be referred to the FinCalc Support Team to change the Users licence, which may have cost implications.

🔓 **Unlocked / Enable User** – If a User’s Profile shows a solid black open padlock, it means that their account is unlocked (available). If the padlock is green, it means that the account is locked. In order to clear a locked account, you simply click on the green padlock to “enable” the User (it will then change to a solid black padlock).

🔒 **Locked / Disable User** – If a User’s Profile shows a solid black closed padlock, it means that the account is locked, and you can choose to unlock it by following the steps above. Alternatively, if the account is not currently locked, the padlock will be green. You have the option to “disable” a User’s account by clicking on the icon and turning it to a solid black closed padlock. This would revoke a User’s access to the system.

🔄

Sometimes a User’s Profile will be colour coded as follows:

Grey – If the User’s details are greyed out it means that the account has been locked.

Yellow – If the User’s details are highlighted in yellow it means that they have exceeded their login attempts and must reset their password. In this scenario, the account remains unlocked.

Red – If the User’s details are highlighted in red it means that they have “shared” their login details with another User and FinCalc has been accessed simultaneously using those login details. This will result in the account being locked.

Further details regarding these colour codes follow in the next Section.

FORGOTTEN PASSWORD/LOCKED RECORDS/SINGLE USER ACCOUNTS

Password Resets/PINs (2-Step Verification)

If a User forgets their password, they have the option to click the “Request new password” button on the login screen. An email will be generated and sent to the User’s registered email address with a reset password link. This link has a default setting of 48 hours, after which a new password reset would be required. As a security measure, upon successful resetting of the password an email is sent to the User confirming the change.

There is a set number of times that a User can attempt to login with their password (as defined by the security settings). If this number of attempts is exceeded, the User is forced to change their password to gain access to the system, as per the above.

Please note that if 2-Step Verification is turned on, a User has five attempts to input the correct PIN (this setting cannot be amended). If the User exceeds five attempts, the User’s account will automatically be locked for security purposes.

Single User Accounts

FinCalc is designed to be used by **Registered Users** and does not allow multiple instances of the same login details being used simultaneously. If an attempt is made to use login details simultaneously, for example on a different computer, the following will happen:

- On the first occasion, both instances will be immediately logged out and a warning message will be shown.
- If this occurs a second time, both instances will be immediately logged out and the account will be locked. If this happens, you cannot unlock that User’s account. You must contact the FinCalc Support Team in order for the account to be unlocked.

CLIENT RECORDS ACCESS & SHARING

Restricted Client Record Access

For Enterprise customers there are two levels of access to client records available.

1. **All Users see all Clients**
2. **Managed User Access to Clients**

With the "**All users see all clients**" option, all Users that hold a chargeable licence will be able to access all client records that are entered on FinCalc and carry out any subsequent actions available, according to their 'User Profile' security settings.

Should a more sophisticated level of client access be required, then the "**Managed User access to clients**" option allows for this. When this option is switched on, Users will only be able to carry out the actions allowed by their 'User Profile' for client records that they have either created, are the owner of or Shared with them.

Additional options are then made available if "Managed User access to clients" is selected:

"**Share Clients at Team Level automatically**" – if selected, this option means any User who has been assigned the same Team as the User who 'owns' the client (see section 8 below) will be given automatic access to the client.

"**Share Clients with Adviser automatically**" – if selected, this option means once an adviser is selected on the Client Profile, that adviser is made the "owner" of the client and the existing "owner" will be made an editor (if they are not an adviser). This option means that the adviser is made "owner" of the client and when used in conjunction with the Team level access, provides an easy way to manage clients at a team level, where Users in other teams are unable to see your team clients.

Roles Associated With Client Records

There are certain roles associated with client records held on the system as follows:

- **Creator/Owner** – the User that created the client record and is the designated owner, unless the owner is changed to the client's adviser
- **Editor** – the User can edit any client record that he/she has access to.

Client Sharing

This feature is specifically for Enterprise users of the software. A client 'Creator/Owner' and or the 'Power User' *(as they can share ownership of any clients as part of their 'User Profile' Settings*) can share access of a client record with another User and make them an "**Editor**". That User can then view the client record and carry out subsequent actions, as per their 'User Profile' Settings.

It is not possible to share access with any Users that hold an IT Admin Profile.

In order to share client rights:

i. On the "Security Settings" screen, the 'Client and Record Access' must be switched to "Managed User access to Clients".

iii. The ‘Sharing Access to Client’ screen details a list of active Users. The non-selectable Users will be greyed out (Users that hold an IT Admin Profile and the client owner (shown in brackets)). Select the Users you wish to Share the client record with by ticking the box next to the Users name. Once you click “OK” it confirms the action. Those members you have selected, then have “Editor” rights.

iv. “Editor” rights can be revoked by going to the Client Profile and clicking on the Share icon and un-ticking the User before pressing “OK”. In this scenario, the User would no longer have any “Editor” rights.

Please note that a Power User has full access to all clients on FinCalc, regardless of which client access mode is in force, and can also carry out all available actions on all clients.

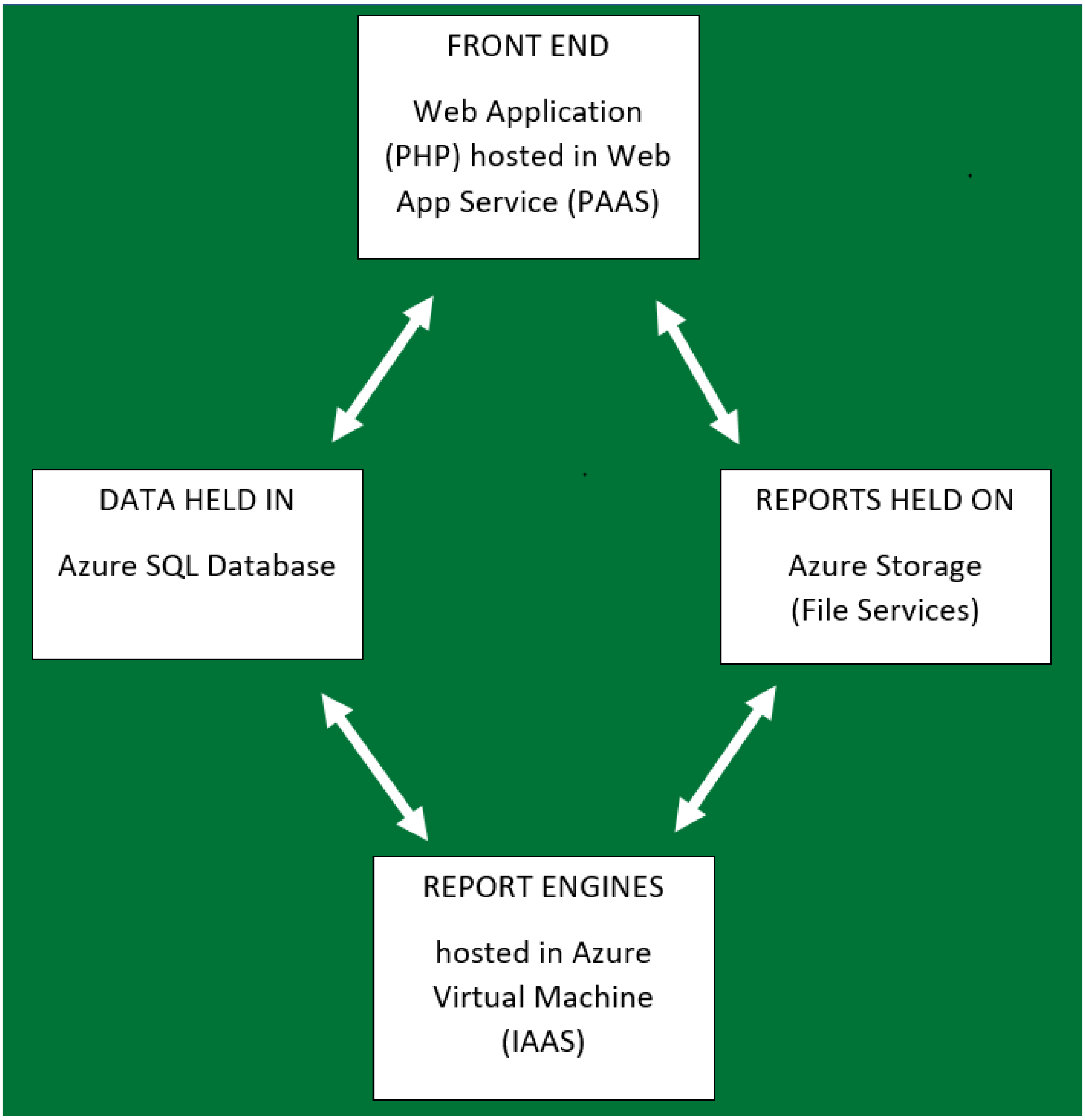
GDPR and Client Data

All data is held securely in Microsoft Azure UK data centres therefore, O&M Pension Solutions Ltd will be classed as Data Processors for your client data. Strict internal controls are in place to ensure only essential access is provided to the SQL data for IT staff and all such access, with timing and reasons, are logged.

Specifically, all data except reports are held within an Azure SQL Database system, whereby Microsoft automatically monitor, manage and patch according to the latest security updates. All data is backed up securely at various intervals during the day and full redundancy of hardware and internet connection to the relevant data centre is taken care of by Microsoft. All SQL data is encrypted at rest and in transit.

APPENDIX 1: WEB APPLICATION NETWORK DIAGRAM

The entire Web Application Environment is hosted in the UK based Microsoft Azure Data Centre.



FRONT END

Web Application (PHP) hosted in Web App Service (PAAS)

DATA HELD IN

Azure SQL Database

REPORTS HELD ON

Azure Storage (File Services)

REPORT ENGINES

hosted in Azure Virtual Machine (IAAS)