FINCALC

Security Q&A

FINCALC
c/o O&M Pensions Solutions
3 The Courtyards, Phoenix Square
Wyncolls Road, Colchester
Essex, CO4 9PE

Tel. 01206 803210
Email. sales@fincalc.co.uk

09/20

Contents

1. About

This document has been created to assist our customers by addressing the security concerns that they may have regarding the FinCalc application.

The FinCalc web application ("FinCalc") is powered by O&M Pension Solutions Ltd ("O&M").

2. Application Access

2.1 Does FinCalc allow for anonymous usage?	No.
2.2 Does FinCalc support single sign on (SSO) authentication?	Not currently. This feature, using SAML 2.0 is now in our roadmap and we expect this to be released by the end of 2020.
2.3 What type of authentication mechanism does FinCalc support?	Email address and password with advanced security features available for customisation by customers.
2.4 Does FinCalc support authentication filtering based on device and/or IP address.	Yes, IP Whitelist functionality is available on the application to restrict access to specific IP ranges. Specific users can be given permission to access the application outside of the IP whitelist (if required).
2.5 Does FinCalc offer an iOS or Android app?	No, it is a web-based application.
2.6 Does FinCalc have any capability on a desktop client for data synchronisation?	No, it is a web-based application.
2.7 Does FinCalc require any software to run on any customer's enterprise server?	No, it is a web-based application.
2.8 Can a user reset their password?	Forgotten passwords can be requested by a user and an email will then be issued to them with a time limited special link to enable the password to be reset. The User's email address must match an active licenced user's email address for the email to be issued.

2.9 What is the default password policy?	The customer can set their own password policy on the application. Please see below for further information regarding the defaults, and the flexibility regarding the level of complexity required for a user's password/login are managed by the customer. 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).

2.10 What is the MFA/ 2FA/ 2-SV policy?	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, if the incorrect PIN is input five times, the User's account will become locked for security purposes (this setting cannot be changed).

2.11 What type of password retrieval methods are used within FinCalc?	All passwords are secured using bcrypt which is a one-way hashing algorithm. All passwords must conform to company set password strength criteria and previously used passwords are not accepted.
2.12 How does FinCalc ensure users only access records that they are permitted to view?	There are two levels of access to client records available to customers. 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 have been Shared with them.
2.13 Can our customers create user roles to fit my business needs?	A range of user profiles are created out of the box and cover most scenarios. Creation of bespoke user profiles is currently on the product road map with delivery expected by the end of 2020.
2.14 Does FinCalc support the automated import of identities?	No
2.15 How do O&M admins access Azure Virtual Machines (VM's) that host the software?	Access VM's is strictly limited and the VM's are secured using JumpCloud (cloud based DAAS) with MFA and further restricted to a specific IP range. We have considered utilising a bastion host, but at this time decided not to implement this.

3. Application Vulnerabilities

3.1 How does FinCalc eliminate Reconnaissance/ Information gathering vulnerabilities?	The application is log in based and a user will only see a generic error page. This is by design so that actual errors are never disclosed. It has also been configured so that search engines will not index the application.
3.2 How does FinCalc eliminate configuration management vulnerabilities?	Various measures are instigated including: - • file extension handling • access to admin interface limited by security permissions • SSL enforced
3.3 How does FinCalc eliminate authentication vulnerabilities?	The application utilises an extensive amount of GUIDs to avoid enumeration risks. Brute force attacks are handled by the system, if the incorrect password is entered more than 5 times the user account is locked. Any password reset instructions are emailed to the registered email address of the user and are time limited. Please see our FinCalc App Security guide for additional information.
3.4 How does FinCalc eliminate session management vulnerabilities?	We have implemented CSRF mitigation to protect against input spoofing. Only secure cookies are used.
3.5 Does FinCalc undertake ongoing DAST tests?	Yes, the latest results of our DAST tests are available for viewing on the due diligence section of our website.
3.6 Is FinCalc FIPS 140-2 validated?	Our Azure SQL database is FIPS 140-2 validated, along with the Report storage. The application is not explicitly validated against FIPS 140-2.

3.7 How does FinCalc eliminate authorisation vulnerabilities?	Various methods are implemented including • path traversal blocked • security permissions limit ability to escalate privileges On every page load the applications re-checks server side that the user has the permissions appropriate to the data that is being displayed on the page. These have been tested by an external pen testing company.
3.8 How does FinCalc eliminate denial of service vulnerabilities?	As mentioned previously, accounts are locked after 5 incorrect login attempts. Admin emails are limited to mitigate DoS attacks. All SQL queries are escaped. Input data is validated before storing against the database.
3.9 Are session timeouts available and can these be customised?	Yes, these are available, and can be customised via the security settings screen.
3.10 How does FinCalc eliminate web service vulnerabilities?	Various measures are implemented including: - • WSDL and SOAP are not used. • Restricted use of Get parameters. • Only 1 trusted 3rd party Rest API is used. • Do not expose our own rest API. • App config limiting to whitelist of external URLs for accessing APIs

4. Data Security

4.1 What type of data would be collected, processed, stored and shared while using FinCalc?	Data is stored in Azure SQL database that is encrypted in transit and at rest. Types of data that may be processed within FinCalc include, without limitation, title, name, date of birth, marital status, spouse's date of birth, address, national insurance number, pension scheme reference number, salary, pension values and other financial data.
4.2 How will the data be accessed, processed and stored?	Data is stored in SQL held in Azure within a UK based datacentre and accessed by the application.
4.3 What is the data flow of the data within the FinCalc application?	On creation of an account for a customer, user details and company information are input to create the FinCalc account. Once the account is established, any further data input into the application is provided by the customer and is stored on Azure datacentre servers within the UK. The customer has the option of deleting information from the application. On termination of the account, the data is held for 30 days and is then deleted from the FinCalc application and the Azure datacentre.
4.4 Is data encrypted in transit to and from FinCalc?	All data is encrypted at rest and in transit to the client.
4.5 Is data encrypted over the O&M's internal network?	Not applicable.

4.6 Is all data-at rest encrypted?	All data is encrypted at rest and in transit to the client. The SQL database uses TDE at rest and can only be accessed via a very limited whitelist of IP addresses. Reports are stored in Azure Storage. Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. Azure Storage encryption is like BitLocker encryption on Windows.
4.7 Is data encrypted on backup media?	Yes, and this is stored only in the UK Microsoft datacentres.
4.8 Is Zero Trust or end-to-end data encryption planned for the FinCalc application?	The final element of end to end encryption (SQL server to web server) is planned for implementation in 2020.
4.9 How are encryption keys managed? Does each cloud consumer have the option to manage their own encryption keys?	The encryption keys are managed in Azure by Microsoft. O&M have an Isolated Managed Environment option available for FinCalc, details of which can be provided on request.
4.10 What is the process for managing the keys?	Keys are refreshed on an annual basis.
4.11 Do O&M administrators have access to view the customer's data in clear text?	No, this is only available at director level and all access is recorded. When the backend is accessed by a Director using SQL Management Studio, they will be able to view data in clear text (except for passwords which are hashed).
4.12 Are there role-based access-granting processes in place to ensure that only the appropriate individuals within O&M will have access to customer data?	Yes

4.13 Does FinCalc store PII (Personally Identifiable Information)? If so, where? How is PII data stored differently from other data?	Yes, this is stored within Azure SQL Database using the same security.
4.14 Will FinCalc protect internal data in transit between services, using correctly configured certificates?	All data is encrypted at rest and in transit to the client. See also 4.8 above.
4.15 Is FinCalc a single tenant or multi-tenant application?	Our application is multi-tenant. We have the option of an isolated managed environment.
4.16 If multi-tenant, what steps have been taken (or will be taken) to secure data from being accessed by other tenants?	Our testing methods for ensuring access to other tenant's data is confidential however our application has been externally penetration tested and at no point were the penetration testers able to access other tenant data.
4.17 What data loss prevention (DLP) capability is built into or integrated with the FinCalc application?	This is built into the Azure infrastructure.
4.18 What is the data retention procedure for FinCalc?	Retained while a customer, securely destroyed 30 days after termination

5. API Information

5.1 Does FinCalc have an API gateway?	This feature is not yet available. Depending on customer demand, this may be introduced in the future.

6. Application Monitoring and Incident Response

6.1 What is our incident response procedure for handling a security or data breach?	In the event of any personal data breach our internal Data Protection Team will investigate and report to the impacted parties within 48 hours of it being identified. We will provide details of what information was affected, how it happened, and any steps taken to mitigate future risk. Additionally, we will inform the supervisory authority (ICO) within 72 hours of the breach being identified. A copy of our Breach Reporting Procedure can be downloaded here.
6.2 Does our incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	Yes
6.3 Is there any alert system to predict or alert on security and other performance issues?	Yes, the system is monitored to ensure it is fully functioning. This is done by monitoring Azure analytical information along with our own internal users testing and using the application ensuring full functionality.
6.4 Do we monitor service continuity with upstream providers in the event of provider failure?	We will get notified by Microsoft if the app is down or performing badly.
6.5 Describe our reporting mechanism for security and/or other incidents. In what format do notifications go out, and what information do they contain?	Data Security breaches will be announced to affected customers via email to the primary contact within 48 hours of identification of such a breach. See our breach reporting procedure mentioned in 6.1 for further information.
6.6 Does our logging and monitoring framework allow isolation of an incident to specific tenants?	Yes

6.7 Do we perform regular vulnerability assessments/penetration tests to determine security gaps?	Yes. Annual penetration tests are carried out against the application, or prior to a significant release. Our most recent attestation report can be found on the due diligence section of the website HERE.
6.8 How long are logs maintained by us? Who has access to the logs?	Logs are held on Azure and these are held indefinitely. Only limited members of senior staff have access to view the logs.

7. Disaster Recovery & Business Continuity

7.1 Do we have written plans for the recovery of all critical applications, platforms, and business function staff related to our customer data and services?	Yes. Whilst the full content of our business recovery plans remains confidential, we regularly test and update these to ensure that we can continue to provide all services to customers.
7.2 What is the guaranteed Service Level Agreement?	Whilst not yet part of our terms and conditions, we aim to add an SLA to our terms and conditions that we will have a 98% service availability with compensation if we don't maintain this. We will update all customers once this has been integrated into our terms and conditions.
7.3 Have we identified the internal systems and services which interface with FinCalc and how a disaster could affect them?	As our application is hosted in Azure, we do not rely on our internal systems to allow our application to function.

7.4 Is there an established BCM policy that has clearly defined roles and responsibilities, is appropriate, maintained, communicated, and documented?	Yes, whilst the full content of our BCM policy is confidential we have written Business Continuity Management Strategies (BCMS) in place which address issues that could arise in the event of any such emergencies. Areas we have covered include: • Our premises becoming unavailable (fire, flood and other events of nature) • Failure of key utilities (power, telephone network, internet access) • Internal Server failure • Staff contingencies (loss of key staff, pandemics and other events of nature) • Emergency contact cascade Should an unforeseen event arise we generally aim to restore full service within 2 working days. We will inform all customers of the disruption as soon as we are aware, ensuring that regular updates are provided in order to keep them informed. This would be done by website message and email. Our BCMS policies are reviewed by Senior Management staff and tested annually to ensure they remain relevant.
7.5 How will you get your data out of FinCalc in a disaster situation, and how you will be able to access your data?	We cannot at this time export customer data on mass from the application.
7.6 What does the disaster recovery plan provide for?	As our application is hosted by Microsoft using their datacentres, Microsoft have extensive disaster recovery plans for power or critical service failure, along with plans for physical disasters such as fire, water damage and flooding.
7.7 Are there business continuity plans for security breaches that could result from the failure of core systems?	Yes, this has been implemented utilising Microsoft Azure.

7.8 In the event of a loss of service, what is the RTO (Recovery Time Objective) for restoring services?	Our RTO would be within 2 business hours. Having tested the disaster recovery on the Azure environment, a full restore took 20 minutes previously.
7.9 In the event of a loss of data, what is the RPO (Recovery Point Objective) for restoring data?	We take a snapshot of the data entered onto the system at the end of each working day. If systems failed during a working day, then the only data that would be lost is that entered on the day of failure.
7.10 What would you do if Microsoft Azure ceased trading for a set amount of time or permanently?	Microsoft would inform us well in advance of any changes to their infrastructure so that we would be able to look for an alternative solution. We are quite comfortable that Microsoft has invested heavily into their Azure infrastructure and will continue to support this indefinitely.