FolioMetrics

Cloud Edition – Cyber Security

Contents

Cloud Edition – Cyber Security

Overview

The FolioMetrics solution is developed using Microsoft technology and hosted on the Microsoft Azure cloud platform which provides FolioMetrics customers with the highest levels of functionality, security and reliability. This document provides an overview of the processes in place to ensure the security of client data stored within the FolioMetrics cloud application.

Hosting Platform Security

The Microsoft Azure platform which hosts the FolioMetrics cloud edition complies with the highest levels of security, resiliency and data protection. Azure is backed by Microsoft's $15 billion investment in global datacenter infrastructure and Azure is continuously investing in the latest infrastructure technologies.

Microsoft Azure security begins with a trustworthy technology foundation. Microsoft designs its software for security from the ground up and helps ensure that the Azure infrastructure is resilient to attack. This is backed by Microsoft centers of excellence that fight digital crime, respond to security incidents and vulnerabilities in Microsoft software, and combat malware.

Microsoft employs intrusion detection, denial-of-service (DDoS) attack prevention, regular penetration testing, and data analytics and machine learning tools to help mitigate threats to the Azure platform. Microsoft anti-malware is used to protect cloud services from malware and viruses.

Further details can be found at the Microsoft Azure Trust Center web site:

http://azure.microsoft.com/en-us/support/trust-center/

Hosting Platform Certifications

Azure has been certified to several key accreditations including:

- ISO/IEC 27001:2005 audit and certification.
- ISO/IEC 27018:2014. Microsoft is the only cloud provider to adhere to the ISO/IEC 27018 code of practice, covering the processing of personal information by cloud service providers.
- SOC 1 and SOC 2 SSAE 16/ISAE 3402 attestations.
- Cloud Security Alliance Cloud Controls Matrix.
- UK G-Cloud.
- EU model clauses.

Further information can be found at: https://azure.microsoft.com/en-gb/support/trust-center/compliance.

Application Security

Further to the security provided by the underlying Microsoft hosting platform it is essential that the application software itself is equally secure. FolioMetrics have ensured that the solution has been designed from the ground up to ensure that it provides the highest levels of security for client data. The application has been designed to be resistant to common attacks including SQL injection and cross site scripting.

Penetration Testing

In addition to the regular penetration testing performed by Microsoft to ensure the security of the Azure platform, the FolioMetrics application itself has been penetration tested by an external security firm to ensure the solution is resilient to common attack methods.

User Authentication

User authentication is provided using Azure Active Directory. As well as providing high levels of security and user management, this also provides the ability for customers to integrate with on premise Active Directory servers and even provide single sign on for users of the FolioMetrics application.

Encryption

All data processed within the FolioMetrics cloud application is encrypted both at rest and in transit.

- Data at rest is encrypted using Microsoft SQL Server Transparent Data Encryption which uses AES-256 encryption.
- Data in transit is encrypted using SSL (https) using a 2048 bit certificate.

Location of Customer Data

FolioMetrics data is stored in Microsoft's European data centers. Within the Europe Azure region, two separate data centers are utilized to provide high availability, even in the event of widespread loss of data center facilities.

The data center locations in Europe are Dublin (Ireland) and Amsterdam (Netherlands).

As well as the inbuilt protection against hardware, network and data center failure, FolioMetrics also provides protection against user error (e.g. accidental large scale modifications) by keeping incremental backups for 14 days.

Segregation of Data

Each client's data is stored within a completely separate database. This ensures the isolation of the information stored by each FolioMetrics client.

Backup of Data

The Azure SQL database solution has built-in data protection, fault tolerance, and data protection meaning that a single hardware failure is automatically handled by the platform. However in addition to this in built protection, additional backups are also made as follows:

- Intraday backups within the primary data centre allowing a point in time restore to any time within the previous 14 days.
- Hourly backup to the secondary data centre to cater for the unlikely event for a major failure of the primary data centre.

Data Retention

Data entered into the FolioMetrics cloud application is always owned by the client. A full backup may be requested at any time. Should a client wish to end its FolioMetrics subscription then a full backup is provided after which the client's data is securely deleted from the cloud service.

FolioMetrics Internal Policies

FolioMetrics has robust internal policies regarding security and access to client data which include:

- Permissions are assigned to employees on a granular basis and access to client systems is only provided to employees who require such access to perform their role.
- Security awareness training is provided to all employees.
- IP restriction and multi factor authentication are utilized where appropriate.