



# Logwise Insider

Logwise insider is a fully managed cloud hosted solution for easy administration of insider lists in accordance with EU Market Abuse Regulation 596/2014. Logwise uses end-to-end best practices for ensuring application security and integrity. All hardware and infrastructural aspects of the Logwise solution use Azure configured services to ensure cutting edge protection and operational stability.

## Secure Managed Cloud Solution

### 100% Cloud Hosted Infrastructure

All server infrastructure, networking, security and OS management is entirely performed by Microsoft based on instructions from Logwise platform experts.

### Fully Managed Solution

Continual updates to the application are included with your contract. No internal IT personnel is required to monitor, diagnose, support or manage any aspect of the solution.

### EU Based

No data leaves the EU at any point in time within the Logwise solution.

### Cutting Edge Security

Logwise Insider is protected by some of the most advanced security measures available today. Your data is secured with multiple levels of military grade encryption and secure authentication mechanism in addition to state of the art threat detection and physical security.



# Security Management

## Azure ISO 27001

Security infrastructure supplied through Microsoft Azure ISO 27001 certified data centers. These data centers are protected by multiple layers of physical security that include perimeter fencing, video cameras, security personnel and secure entrances. This multi-layered security model is in use throughout every area of the facility, including each physical server unit.

Logwise uses Azure services to establish a Secure Perimeter around the Logwise solution using secure networking, internal virtual networks, firewall protection, malware protection, threat analysis and detection with advanced security analysis algorithms and continual security analysis provided by Microsoft's Cyber Defense Operations Center and Azure Security Analysis Services.

## SQL Encryption

All databases use encryption for at-rest storage using AES 256 and in-transit encryption using SSL/TLS. Asymmetric keys used for transparent data encryption of database files are fully managed by Microsoft and keys are automatically rotated every 90 days.

## Encrypted Data Transfer

All communication between servers and services that make up Logwise Insider is fully encrypted both within the Azure Secure Perimeter and for all incoming/outgoing data.



## Identity & Access Management

### Multi Factor Authentication

All operations access to the Logwise production environment requires admins to login using both their Azure AD account and to approve logins simultaneously on a trusted personal mobile device.

### Conditional Access

Azure AD monitors account usage to block suspected use of any operations accounts independently of the Logwise administrators manual intervention.

### Administrator Password Management

For security reasons Logwise staff are not able to reset lost passwords for their own Azure AD accounts. In the event of an administrator account being locked out due to suspected use or forgotten passwords the user cannot automatically reset their password. A different AD administrator is required to reset the password and provide a one-time password by SMS.

### Administrator Password Policy

Critical passwords are changed on a 70 day schedule. Non-critical passwords are rotated on a 120 day schedule. No password duplicates are allowed and password strength is enforced. Every user accessing Azure services does so using a personal account with MFA enabled. Passwords are never stored or transmitted in clear text. A client based encrypted password storage system is provided for administrators to store passwords securely if storage is required. This also provides a rules based emergency password access facility in the unlikely event that an administrator with specific access rights is taken sick for an extended period.

### User Password Management

No clear text passwords are stored for end-users of the service, all passwords are stored as salted SHA256 hash values in a separate database from client data. Authentication is provided using an Azure hosted STS using OAuth 2.



## Information Protection

### Database Backup

Continual point-in-time backups allow restoring the database to any point in time in the last 7 days. Database logs are backed up every 5 minutes, differential backups are performed every day and full backups are scheduled on a weekly basis. All backups are transparently encrypted to protect from unauthorised use.

### GDPR

All data is stored and managed in accordance with EU General Data Protection Regulation 2016/679. Logwise acts as your Data Processor for insider lists and a legal agreement is setup between your company and Logwise to ensure compliance with GDPR. Logwise does not have any legal right to use the information that is stored in your insider lists and no information is provided to third parties other than when you send insider lists to your National Financial Regulatory Authority in accordance with the requirements of MAR.

### Encrypted Email

Logwise provides a secure email delivery service for communicating with insiders, administrators and as required your National Financial Regulatory Authority. All emails are sent over an encrypted email service provided by Google one of the world's leading and most trusted email providers. Emails sent to insiders are encrypted at the transport level, no message level encryption is used by default for insider emails so that no complex client-side configuration is required. Emails sent to National Financial Regulatory Authorities are encrypted as required by those Authorities without any setup or intervention required on your side.

### Client Data Masking

During day to day monitoring and operations no customer data such as project names, insider emails or personal details are exposed to Logwise staff - all data is masked inside the database returning "email\*\*\*\*\*" or "name\*\*\*\*\*" instead of real data. This allows Logwise staff to monitor database operations and integrity without gaining access to any sensitive data that may be stored in the system.



# Threat Protection

## Azure Cyber Defense Operations Center

A global 24/7 team of over 3500 Cyber Security experts monitor and defend the Azure Cloud Platform from cyber threats. Microsoft invests in excess of \$1 billion dollars annually in security on their platforms and services.

## Cloudflare DDOS

Logwise utilises Cloudflare Anycast DNS network and advanced DDOS analysis and protection built to overcome global denial of service and volumetric attacks at multiple levels (Level3/4, Level7 & DNS). Continual traffic based threat analysis with multiple levels of defence responses ranging from Captcha challenges to blocking network requests with massive scale able to mitigate attacks in excess of 500 Gbps.

## Backup Anycast DNS

In the event of a catastrophic failure at Cloudflare a secondary DDOS resistant Anycast DNS network is continually available to provide Domain Name resolution.

## Emergency Data Center Switch

Should the Logwise primary Azure data center become inaccessible. Microsoft or Logwise personnel as determined by the outage will initiate a switch to one of multiple alternate data centers within the EU.

## Security Monitoring

All access to Logwise production Azure resources are monitored and audit logs are automatically and manually analysed to detect illegitimate patterns and unauthorised access. All changes to the Azure production environment results in instant email and SMS messages to key Logwise personnel to ensure that breaches of the Azure management accounts do not go undetected.

## Malware, XSS & SQL Injection Protection

Constant malware monitoring is performed on all parts of the Azure infrastructure. Logwise Insider is designed to not allow Cross Site Scripting or SQL Injection attacks.