MindaClient Security & Data integrity

ISO 27001 Certified

- MindaClient is very proud to announce that in May 2026 we have successfully been ISO 27001 certified. Since we were established in 2002, we have always focussed on data security, reaching this globally recognized milestone takes that commitment to the next level. This certification is a reflection of our continuous investment in protecting your most valuable asset your data.

- ISO 27001 is the world's most widely recognized standard for Information Security Management Systems (ISMS). It was developed by the International Organization for Standardization and it sets out the framework a company needs to establish, implement and maintain rigorous information security processes. To achieve this, we underwent extensive, independent auditing of our systems, infrastructure and internal processes across two stages of external auditing.

-

Intrusion Detection and Prevention

- A dedicated hardware firewall is deployed at the network perimeter to filter incoming and outgoing traffic.
- A software firewall is installed on the web server to control traffic at the application layer.
- A web application firewall (WAF) is configured on the web server to detect and mitigate attacks targeting web applications.
- On top of the server level firewall, the server also monitors SSH, POP, IMAP, SMTP, FTP for failed logins or Mod Security WAF hits. This blocks IPs based on the thresholds set. We add known blacklisted IPs automatically. We also have external detection and mitigation on the network for volumetric DDOS attacks.

Data Backup

- The MindaClient database is backed up automatically every 60 minutes, 24/7.
- Backups are transmitted and encrypted between the primary server and backup storage to ensure data integrity and confidentiality during transit.
- The service features a robust error monitoring system that reports on each backup operation. If any errors arise during the backup process, administrators are promptly informed, allowing for swift intervention and issue resolution.
- Backups are encrypted at rest

Anti-Virus / Anti-Malware

- Top-tier antivirus and anti-malware software is installed on the web server for real-time scanning and detection of malicious activity.

Failover

- We use real-time data replication and server-to-server synchronisation to maintain an independent failover of the MindaClient service. In the event that the primary. MindaClient server becomes unavailable, we have the facility to use IP switching and failover to our secondary system in order to maintain availability.
- Our failover is hosted on the AWS Cloud

Authentication

- The system implements robust authentication protocols to ensure secure user identity verification.
- Access control mechanisms restrict system access exclusively to authenticated and authorized users.
- Users are granted access permissions based on assigned roles, with restrictions applied at both functional and data access levels.
- All user passwords adhere to strict complexity requirements, meeting strong password standards for uniqueness and entropy.
- Data transmission between client and server is encrypted using HTTPS, ensuring confidentiality and integrity of data in transit.
- The system supports enforced password rotation policies, allowing administrators to mandate periodic password changes.
- User authentication requires a unique identifier (username as a verified email address) combined with a strong password.
- Each authentication event is logged with a precise timestamp, and these logs are securely stored in an audit trail for tracking purposes.
- Administrators have read-only access to audit logs of all user authentication events for security monitoring.

Two Factor authentication

- Multi-factor authentication (MFA) is available for MindaClient accounts, utilizing a two-factor authentication (2FA) solution via time-based, one-time passcodes (e.g., Google Authenticator) to enhance account security.

Forced Password Expiration

- Administrators can configure password expiration policies by setting custom time intervals for mandatory password changes. For example, users can be required to update their passwords every 90 days to enhance security compliance

Password Recovery Process

- A secure, self-service password recovery and reset mechanism is provided, utilizing a two-step authentication workflow to securely reset user credentials.
- This feature is accessible to users with specific roles, including administrators, applicants, and reviewers.

Authorisation and role-based security

- The MindaClient platform incorporates predefined roles/personas designed to meet various access and security requirements. These roles include:
    - Overall Administrator
    - System Administrators
    - Ordinary Administrators
    - Read-Only Administrators
    - Application Reviewers
    - Applicants
    - Mobile-Only Users
- The platform enforces both functional and data-level restrictions, allowing administrators to assign access to specific locations or datasets based on user roles.
- An Administrator GUI provides an intuitive interface for managing and updating user permissions, enabling precise control over role-based access.

Audit Trail

- All data modifications are systematically recorded and stored within the audit trail of the system. A streamlined interface is provided to query the audit history of all data related to a specific client.
- Administrators have the ability to review the audit trail for both individual clients and applications. The audit reports detail the original value, the modified value, the user responsible for the change, along with the date and time of the modification.
- Audit trail records can be filtered by date range and staff member.

Data retention & archiving

- The system supports the secure storage and archival of all received documents.
- Data can be bulk transferred to an archive by updating the status of the records.
- In accordance with your GDPR policy, bulk deletion of data that is no longer required is also supported. Our GDPR module enables data searches using a combination of client filters, date filters, and permission filters to identify data that should be deleted. Once identified, this data can be securely deleted.
- To prevent accidental deletion, several safeguards are in place, including requiring the administrator to manually enter the word "Delete" before the action can be performed.

Hosting

- Our servers are all located within the EU, including all offsite backups and failover services. The data centre we use has Tier III data centre classification and ISO 20000 / 9001 / 14001 / 27001 certified.
- The system will be hosted in Dublin, Ireland. Backups are stored within the EU. The data storage is in compliance with GDPR requirements