MindaClient Security

1. **Intrusion Detection and Prevention**
   The system employs a combination of hardware, software, and web application firewalls alongside top-tier real-time antivirus, anti-malware, and external detection tools to continuously safeguard the server from threats.

2. **Data Backup**
   All servers within our network are backed up hourly, with backups encrypted both in transit and at rest. The backup process is continuously monitored.

3. **Failover**
   We use real-time data replication and server synchronization to ensure continuity. Failover services on AWS Cloud use IP switching to minimize downtime.

4. **Encryption of Personal Data in Transit**
   All data transferred between clients and the server is encrypted using HTTPS to ensure confidentiality and integrity.

5. **Authentication and Multi-Factor Security**
   Access is restricted to authenticated users, with strong password policies, enforced password rotation, and multi-factor authentication (MFA) using one-time passcodes for enhanced security.

6. **User Access Control Management**
   We enforce strict control over server access, limiting it to authorized users, specified networks, and designated devices.

7. **Data Retention and Archiving**
   Data is securely stored, archived, and deleted in compliance with GDPR policies. Safeguards prevent accidental deletion, ensuring only authorized actions are performed.

8. **Software Updates**
   Updates and security patches are installed regularly by the server management team to ensure the integrity of our software.

9. **Data Centre**
   All servers are housed in Irish data centers with Tier III classification and ISO certifications, ensuring high standards of security, quality, and compliance. Backups are always maintained within the EU.