MindaClient Security

1. **Data Centre**
   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.

2. **Firewall**
   Our MindaClient server is protected by physical and a software firewalls. Traffic on all ports is tightly restricted. Access, where appropriate, is locked down by IP address.

3. **User Access Control Management**
   Access to the server is severely limited. Only the MindaClient Development team have access the server or the database. Direct access to the server is restricted to our office IP address, and a strong password policy is observed. Our server management company may also, with our permission, access the server to perform upgrades and server administration.

4. **Password Policy**
   It is the policy of SalesPulse / MindaClient that all passwords are unique, and complex (meeting the 'strong password' standard). All passwords are changed on a monthly basis.

5. **Software Updates**
   Updates and security patches are installed regularly by our server management team.

6. **Encryption of Personal Data in Transit**
   All data transferred to and from the website is encrypted via HTTPS.

7. **Intrusion Detection and Prevention**
   On top of the server level firewall, we use CSF Firewall to monitor SSH, POP, IMAP, SMTP, FTP, for failed logins or Mod Security WAF hits. This also blocks IPs based on the thresholds set. We also add know blacklisted IPs automatically. We also have external detection and mitigation on the network for volumetric DDOS attacks.

8. **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.

9. **Data Backup**
   The MindaClient database is backed up automatically every 60 minutes, 24/7. The backup is from secure web server to secure web server over SSH, so all data is fully encrypted end to end during the backup process. The backups are accessed through a secure portal using a strong password.