Adaptive Business Management Systems – Security Profile

Effective Date: October 3, 2025 (updated)

Executive Summary

At Adaptive Business Management Systems Ltd (Adaptive BMS), protecting customer data is our highest priority. We recognise that our customers operate in highly regulated industries (including aerospace, medical devices, pharmaceuticals, oil & gas, and manufacturing), and we design our security measures to meet and exceed global standards.

We secure your information through:

- Accredited UK data centres (ISO 27001, ISO 9001, ISO 14001, PCI DSS).
- Encryption of all data in transit (TLS/SSL) and at rest.
- Strong authentication controls, including two-factor authentication and login monitoring.
- Continuous monitoring, logging, and threat detection.
- Regular backups, disaster recovery planning, and tested recovery processes.
- Ongoing staff training and internal ISO 27001-aligned audits.
- Regular vulnerability scanning and penetration testing.

These controls ensure resilience, compliance, and the highest levels of trust in our products and services.

About Adaptive BMS

- Over a decade of experience in digital corrective and preventive action systems.
- Creator of CAPA Manager, a leading cloud-based solution for issue management and investigations.
- Founded by quality professionals, with security and compliance built into our DNA.

Compliance & Standards

We align our processes with globally recognised standards:

- Internal audits: conducted against ISO 27001:2013.
- Data centre suppliers: hold accreditations including ISO 27001, ISO 9001, ISO 14001, PCI DSS.
- Data protection: we comply with the UK Data Protection Act 2018 and EU/UK GDPR.

Infrastructure Security

Corporate offices: Dorset, UK.

Primary hosting: Two independent Tier 3+ data centres in Manchester, UK.

- 24/7/365 on-site engineers.
- Redundant UPS and diesel generators.
- Fire suppression and VESDA early detection systems.
- Strict physical access controls.

Data Protection & Encryption

- In transit: All traffic is encrypted via HTTPS/TLS using Extended Validation SSL certificates (2048-bit key, 256-bit encryption).
- At rest: Databases, applications, and backups are encrypted using industry best practices.
- Authentication: All user credentials are encrypted immediately on creation and stored in hashed/encrypted form.

Access Management

- Internal systems:
  - Two-factor authentication (2FA) mandatory.
  - Role-based access control (least privilege).
  - Access revoked when no longer required.
- Applications (customer-controlled):
  - Password complexity enforcement.
  - 2FA with location/IP recognition.
  - Failed login attempt lockout.
  - Session monitoring and automated re-challenge.

Operational Resilience

- Backups:
  - Application and customer data backed up to remote secure locations.
  - Customer backups retained securely for 6 months; application backups until end of useful life.

- Disaster Recovery (DR):
  - DR plan tested regularly.
  - Services can be restored to alternate sites within 72 hours in case of full site loss.
- Incident Response:
  - 24/7 monitoring and alerting systems.
  - Incidents classified and contained immediately.
  - Root cause analysis and corrective actions implemented.
  - Customer notification within 72 hours if personal data is affected (GDPR standard).

Threat & Vulnerability Management

- Regular patching of infrastructure and applications.
- Automated vulnerability scanning and manual security reviews.
- Multi-layer threat detection, including intrusion monitoring and behavioural analytics.
- Independent penetration testing available annually or on request.
- Customers may conduct authorised penetration testing with prior arrangement.

Logging & Monitoring

- All infrastructure components generate security logs (firewalls, routers, load balancers, operating systems, and applications).
- Logs are continuously monitored, with alerts for:
  - Excessive login attempts.
  - Privilege escalation or manipulation.
  - Behaviour outside established baselines.

Malware Protection

- Comprehensive anti-malware technology deployed across infrastructure.
- Continuous scanning of files, attachments, and applications.

People & Training

- Dedicated Security & Compliance team, with oversight from company leadership.

• All employees undergo mandatory security and GDPR training at induction and annual refreshers.

• Functional business units (Support, Development, Sales, IT, Training) have clearly defined security responsibilities.

Data Handling & Customer Rights

• Sensitive data: Customers may store confidential information but not payment card details (PCI DSS restricted).

• Data export: Customers can export data at any time. Full database export available on request.

• Data deletion: Upon termination, data is securely deleted (rendered unrecoverable). Written confirmation available if required.

Commitment to Continuous Improvement

Security is not static. Adaptive BMS continually invests in people, technology, and processes to:

• Anticipate and defend against emerging threats.

• Improve resilience and availability.

• Maintain compliance with evolving regulations.

Contact

For security enquiries:

Data Protection & Security Officer

Adaptive Business Management Systems Ltd

📧 support@adaptivebms.com