Security Profile
Adaptive Business Management Systems Ltd.

Updated: Effective on May 26, 2020

About our organization

Adaptive Business Management Systems Ltd. has more than a decade of experience providing organizations around the world with comprehensive issue management and investigation software.

Originally formed by a handful of quality professionals to digitize their paper-based corrective action systems, the team started sharing the original product ‘Key Task Monitor’ (KTM) for free with other quality professionals. Due to popular demand, the original KTM product was further developed into the commercially available product available today, CAPA Manager. Due to the practical origins of the CAPA Manager product, it has become one of the most popular corrective action products available.

We are committed to the responsible operation of our organization and we maintain high values of customer focus and operational quality. We understand that security is of the highest priority to our customers, we also understand that our customers rely on us to manage and develop our security-related features and processes.

This document is about how we approach security

This document describes security controls, policies and procedures deployed within our organization and within our critical infrastructure suppliers.

Compliance

We work to a comprehensive set of operating standards demonstrating our commitment to data security, privacy and conformance to applicable regulations.

Internal management systems

We regularly perform our own internal audits for compliance in accordance with the following standard:

- ISO 27001:2013

Critical infrastructure suppliers

Our data centre suppliers hold accreditations for:

- ISO 27001
- ISO 9001
- ISO 14001
- PCI DSS

Security Profile
Adaptive Business Management Systems Ltd.

Updated: Effective on May 26, 2020

Technical overview

Corporate infrastructure

Our primary management base is located in Dorset, United Kingdom.

Physical infrastructure

Server hardware is located in two specialist data centres in Manchester, United Kingdom. The physical server infrastructure is managed and supplied by a specialist provider.

Our data centres feature skilled, 24x7x365 onsite engineers, redundant N+1 UPS and N+1 diesel generators, fire suppression and VESDA detection systems.

Both data centre facilities have leading accreditations (ISO 27001, ISO 9001, ISO 14001, and PCI DSS) and best practice security and access controls.

Disaster recovery summary

Our systems, data storage and applications are regularly backed up in remote locations. We can recover quickly in the event of unforeseen disasters. We can move our digital services to alternative recovery locations should this ever be needed.

Monitoring and analytics

We use a variety of monitoring and analytical tools to:

- Find and fix errors within our products and services
- Improve end-user experience
- Understand customer engagement with our products and media
- Monitor overall application performance
- Assist with specific customer issues

Access management (user authentication)

Internal electronic systems

Two-step authentication is required to access all company applications, tools and data. Strict access management applies to all direct and indirect employees.

Adaptive Business Management systems Ltd. allocates access on an ‘as needed’ basis. If access isn’t required then access is revoked.

Security Profile
Adaptive Business Management Systems Ltd.

Updated: Effective on May 26, 2020

Applications and products

The following security mechanisms are available in all our products requiring access control, these are configurable by the customer.

- Password complexity
- 2 step authentication
- Failed login attempt banning

Password complexity (customer-controlled)

Password complexity requirements can be enforced. A minimum number of upper case characters, the minimum number of lowercase characters, the minimum number of digits, the minimum number of special characters, minimum length, expiry.

2 step authentication (customer-controlled)

If the user's physical login location changes, the CAPA Manager application will recognise this and further steps will be needed to verify their identity. They will be emailed a secret code to confirm that the login attempt is valid.

Failed login attempt banning (customer configured)

Failed login attempts will result in an application access ban or recapture authentication.

Encryption of data transfer

All data transmitted to and from our web-based products are encrypted using a commercially purchased SLL (Secure Socket Layer) key. Our data encryption controls include:

- All application traffic transits over encrypted HTTPS channels
- 2048-Bit extended validation SSL, 256-Bit Encryption
- Extended Validation encryption certificates are issued by premium Certificate Authorities

Data at rest security

Access to the application and database tiers are protected by multiple active and passive security systems:

- Ultra password complexity
- 2 step authorisation mandatory
- Location and IP address control
- Aggressive failed login attempt banning
- Automatic user activity monitoring (virtual recapture)

Security Profile
Adaptive Business Management Systems Ltd.

Updated: Effective on May 26, 2020

Security policies and procedures

Governance and risk management

Adaptive Business Management Systems Ltd is responsible for directing and controlling operations and for establishing, communicating and monitoring policies, standards and procedures. We achieve operational and strategic compliance with the company's overall objectives through proper preparation, planning, and execution.

High importance is placed on maintaining strong internal controls, and the ongoing training of all personnel.

Responsibility and accountability for the design, development, implementation, communication and maintenance of security and availability policies are assigned to different teams within the organization. These teams operate under the oversight of our leadership team in accordance with our agreed strategy.

People and training

Adaptive BMS is segmented into functional units:

- Customer support
- Finance
- Research and development
- Sales
- Security and compliance
- Special projects
- Training
- IT and infrastructure

Each business unit is led by a functional leader who is also part of the leadership team. The leadership team actively supports information security within the organization. The leadership team demonstrates its commitment to data security through, strategy, planning, and continual review of our information security responsibilities.

We are committed to training and developing our employees, commencing with initial training on data security. All employees have a defined training plan which supports business strategy and employee personnel development.

Standard training includes information and data security, quality values and operating practices.

Security Profile
Adaptive Business Management Systems Ltd.

Updated: Effective on May 26, 2020

Operational resilience

Backups

Adaptive Business Management Systems Ltd maintains a data backup and restoration process to recover from data loss events. Data is backed up to remote digital locations on a weekly basis.

- Customer data backups are securely destroyed after six months
- Application backups are kept until their useful life has expired

Disaster recovery

Our Disaster Recovery strategy addresses the physical loss of our data hosting locations and management offices. It is estimated that full services would be restored within 72 hours in the event of a total loss of the current hosting infrastructure.

Incident management

We follow a formalized security incident management process to evaluate and provide timely response to security incident and event notifications. Incidents are triggered from a variety of sources including:

- Automated monitoring and alerting tools
- Cybersecurity diligence from threat bulletins, news wires and vendor statements
- Direct notifications from employees, customers and other stakeholders
- Management surveillance and oversight of compliance to policies and procedures

Our response activity is proportional to the situation or risk presented:

- Define: Record and capture all details about the issue
- Contain: Take all appropriate steps to:
    - Prevent the issue from getting worse
    - Fix the issue for our users
    - Provide the required information to affected stakeholders (internal and external) as appropriate
- Root cause: Understand the cause of the issue
- Rectify: Make process changes to prevent the issue from happening again

Security Profile
Adaptive Business Management Systems Ltd.

Updated: Effective on May 26, 2020

Security controls and lifecycle management

Datacenter security (Physical infrastructure security)

Both our data centre facilities have leading accreditations (ISO 27001, ISO 9001, ISO 14001, and PCI DSS) and best practice security and access controls.

Threat and vulnerability management

Adaptive Business Management Systems Ltd. uses a multi-layer approach to identify potential threats that would impair system security and availability. Multiple automatic applications are used to protect against potential threats. Threats and vulnerabilities are identified by means of:

- Regular automated patching of all software, systems and applications
- Automated and manual scanning of infrastructure and underlying components
- A commitment to continually develop and improve our software security systems

Event logging

All infrastructure components including firewalls, routers, load balancers, operating systems and applications send log information to enable security reviews and analysis. Certain activity types trigger automatic alert notifications to hosting provider and our own information security teams, including:

- Excessive login attempts
- Manipulation of privileged accounts or security groups
- Behavioural activity outside of baselines

Anti-malware

We use comprehensive anti-malware technology to actively scan systems, files and software for malicious files and attachments.

Sensitive data

Our software products are used by customers in a variety of ways, customers may choose to hold confidential and/or protected data within the system. We do not interactively manage data within customer systems, we apply our information security policy and procedures equally across all customer data.

Note: Customers are not permitted to use our products to hold payment card data, authentication data, or credit or debit card numbers.

Security Profile
Adaptive Business Management Systems Ltd.

Updated: Effective on May 26, 2020

Returned data

As part of the customer disengagement process, customers may request a copy of their data. We can facilitate such requests (at cost) by providing a copy of a customer database in an industry-standard format. Customers maintain the capability within the platform to export partial or complete data at any time.

If Adaptive Business Management Systems Ltd. is asked to provide data directly, then there may be a charge for this service.

Data deletion

At the conclusion of our relationship with a customer, after the default retention period, data is deleted in such a manner so as to be unrecoverable. Customers may request written confirmation of this deletion should they so choose. Customers can request immediate deletion of data if needed.

User authentication

When issuing login credentials for access to any of our products, authentication consists of standard username and password. Authentication credentials are encrypted immediately and stored in an encrypted state, each with a unique key.

When a password expires, users will be prompted to update their password.

Vulnerability and penetration testing

Adaptive Business Management Systems Ltd participates in vulnerability assessments and penetration testing of its software products. These reviews are usually conducted in-house as part of our regular software development process. We can facilitate testing by 3rd party providers if needed.

Customers can perform their own penetration testing on a scheduled basis with prior agreement. An identical system can be provided for this purpose.

We actively address any potential vulnerabilities before any exploitation can occur.