

Midaxo Cloud Security Whitepaper

2025-12

Classification: Public

Executive Summary	3
Introduction to Midaxo Cloud	3
Governance & Compliance	3
Information Security Management System.....	3
Infrastructure Security Architecture.....	6
Cloud Platform Foundation.....	6
Shared Responsibility Model	7
Network Security	7
Identity & Access Management.....	8
Authentication Framework.....	8
Access Control and Authorization	9
Data Security & Privacy	9
Data Governance	9
Data Protection.....	10
Application Security.....	11
Secure Software Development Lifecycle.....	11
AI Security & Governance.....	12
AI Integration Architecture	12
AI-Specific Security Controls	13
AI Governance.....	13
Threat Detection & Monitoring	15
Security Operations Monitoring	15
Vulnerability Management	15
Incident Response & Business Continuity	15
Incident Management.....	15
Business Continuity Measures	16
Service Status Communication	16
Physical & Environmental Security	16
AWS Data Centers	17
Midaxo Offices.....	17
Change & Release Management.....	17
Change Management Process	17
Software Development Process	17
Version Control and Release Authorization.....	18

Third-Party Risk Management 18

Supplier Selection and Management..... 18

Third-Party Component Management 18

Asset Management..... 18

Human Resources Security 18

Disclaimer, Trademark and Copyright Notices..... 19

Executive Summary

Midaxo is committed to maintaining a high level of information security, with protecting customer information as its key priority.

The certified Midaxo information security management system (ISMS) complies with ISO/IEC 27001:2022 and AICPA's SOC 2 requirements. Security controls are designed based on risk analysis, with periodic risk management performed throughout the organization to ensure mitigation of emerging threats.

The technical implementation has been designed to meet strict customer security requirements and industry best practices. The architecture protects data both in transit and at rest, ensuring confidentiality, integrity, and availability through comprehensive security controls.

Documented processes and continuous monitoring ensure timely incident response. Independent third-party audits and penetration testing verify that information security meets the highest standards.

Introduction to Midaxo Cloud

Midaxo Cloud helps Corporate Development teams to perform their business processes, such as mergers and acquisitions (M&A), divestments, various rationalization processes, and partnership models in a defined, systematic way.

Midaxo Cloud provides an enterprise-wide workspace, where different business processes and their projects can be managed efficiently.

Governance & Compliance

Information Security Management System

The information security management system has strategic importance to Midaxo, as Midaxo recognizes the importance of information security and confidentiality in the field of Corporate

Development and M&A. Midaxo's information security management system is an integrated part of Midaxo's day-to-day operations and governance covering Midaxo's personnel, processes, and systems.

Policies for Information Security

Midaxo has internal information security policies defining Midaxo's security requirements and controls. Employee awareness is ensured through new employee induction and regular training thereafter. The policies are reviewed at least annually and approved by Midaxo's management team.

Roles and Responsibilities in Information Security

Midaxo's management team sets targets for information security and regularly reviews their status. The management team acts as an information security steering group. Midaxo's CISO is responsible for information security management.

Certifications & Audits

Midaxo has ISO/IEC 27001:2022 Information Security Management certification. ISO 27001 is an internationally recognized security management standard that specifies security management best practices and comprehensive security controls.

Midaxo Cloud has completed the System and Organization Controls (SOC) SOC 2 Type 1 audit and is in progress to complete the SOC 2 Type 2 audit by Q2 / 2026. The SOC 2 audit complements Midaxo's ISO/IEC 27001:2022 certification and validates further the effectiveness of the security controls.

Midaxo Cloud is regularly penetration tested by independent information security expert services companies. Customers and prospects can download the latest attestations and certificates from Midaxo's website. The independent penetration testing verifies that the Midaxo Cloud architecture and software are designed, implemented, and maintained securely. Other independent third-party auditors and expert service companies regularly audit Midaxo Cloud's security.

Midaxo offers customers the opportunity to perform security audits and penetration testing of their own with a staging instance with the same architecture as in Midaxo Cloud's production environment.

AWS Platform Certifications & Audits

Amazon Web Services platform security is proven by the following certifications and audits:

- SOC 1/ ISAE 3402, SOC 2 and SOC 3
- Cloud Security Alliance (CSA) STAR registrant, and has completed the CSA Consensus Assessments as well as the Initiative Questionnaire (CAIQ)

- PCI DSS Level 1 compliance
- ISO 27001 Information Security Management and ISO 9001 Quality Management certification

For more information about Amazon cloud platform security, visit the [AWS Security Center](#).

Risk Management

Internal and external risk analysis is performed regularly. Identified risks are managed with risk treatment plans. Policies and processes are continuously improved based on the risk analysis findings.

Personal Data Processing

Midaxo's practices for collecting, processing, protecting, and disclosing personal data are detailed in Midaxo Cloud's [Privacy Policy](#).

The following personal data are processed and stored in Midaxo Cloud:

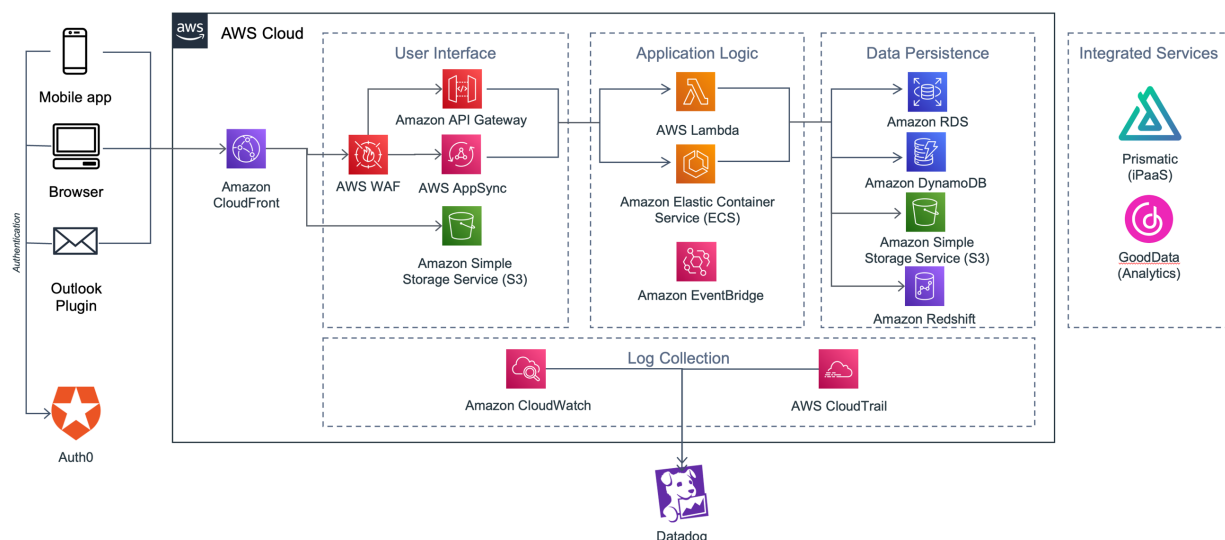
- First and last name
- Work email address
- IP address

For additional information on compliance provided by Amazon Web Services, see [AWS Compliance](#).

Infrastructure Security Architecture

Cloud Platform Foundation

Midaxo Cloud runs on Amazon Web Services' (AWS) leading cloud platform, utilizing the AWS Serverless Computing. With serverless computing, infrastructure management tasks like capacity provisioning and patching are handled by AWS.



Midaxo Cloud environment contains several distinct layers of services:

User Interface Layer

Hosts a React based Single Page Application (SPA) that embeds other SPAs in the main Single Page Application. This application is hosted on Amazon S3 as a static site and has an Amazon CloudFront content distribution network (CDN) provisioned in front of it.

Authentication Layer

Fully managed by Auth0 and is integrated to the User Interface layer through Auth0's SDKs and the API layer is configured to trust only tokens issued from the Midaxo Cloud's Auth0 tenant.

API Layer

Has an AWS AppSync GraphQL & Amazon API Gateway endpoint provisioned that use AWS Lambda based functions to read and write from the Data Persistence layer. AWS Lambda functions are implemented in Python programming language. API layer publishes events to Amazon EventBridge for communication across the different services within the API layer.

Data Persistence Layer

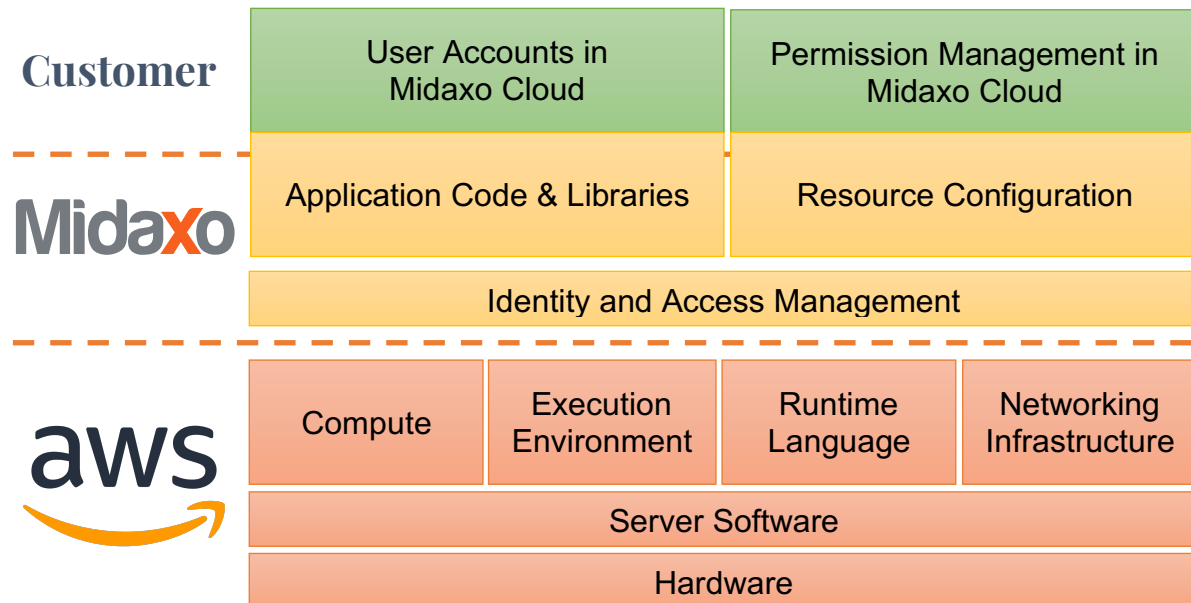
Stores the data in Amazon RDS relational database, Amazon DynamoDB NoSQL database and uploaded files are stored in Amazon S3.

Log Handling Layer

Uses Amazon CloudTrail and Amazon CloudWatch Logs to ship the logs for processing to Datadog. Datadog provides a centralized logging service for Midaxo Cloud.

Shared Responsibility Model

In cloud computing, Security and Compliance is shared responsibility between AWS and Midaxo. Midaxo is responsible for the security of the actual application code and libraries, AWS resource configuration, and for identity and access management to manage these resources. Customers are responsible for managing the access to their Midaxo Cloud workspace, including user accounts and permission management.



Network Security

As described in the shared responsibility model, the networking infrastructure for Midaxo Cloud is responsibility of AWS. Midaxo is responsible for configuring the access to different services utilizing AWS tools.

Firewalls

All communication to Midaxo Cloud goes through AWS Web Application Firewall. Midaxo Cloud's internal network is separated into different subnets, which have their own network

access control lists to limit allowed traffic. Security groups with allow rules using other security groups as sources are used to micro-segment allowed traffic on cloud resources.

Monitoring

All AWS Services, including Web Application Firewall, are monitored 24/7 basis with Datadog security monitoring. Network activity logs are captured and retained.

Segmentation

To ensure network security, the Midaxo office network that is used for administrative work is segregated from the Midaxo Cloud production environment. Separate quality assurance and staging environments are used for testing. These environments are segregated fully from the production environment.

Identity & Access Management

Authentication Framework

To access Midaxo Cloud, users are authenticated either with username and password, or with Single Sign-On using their identity provider. Supported SSO protocols are SAML 2.0 and Open ID Connect (OIDC).

Authenticated users get a security token to identify them. The token exchange uses the Authorization Flow with PKCE that secures the security token retrieval. In each request to the Midaxo Cloud API layer, the security token is checked. Based on the security token, a user can be authorized. As the tokens are critical for user authentication and authorization, they are short-live to reduce the risk from their exposure.

Authentication Management

Midaxo Cloud uses Auth0 for authentication and authorization. Auth0 locks a user account after a defined number of failed login attempts. If a session is idle for 2 hours, it will expire automatically and require the user to log in again. Each session must reauthenticate again after 8 hours.

Password Policy

Midaxo Cloud enforces a strong password policy, which requires 12-character long passwords at minimum and passwords containing mixed case characters, including special characters. Midaxo Cloud has requirements for end-user password length and complexity. Passwords are hashed and then stored in the Auth0 database. Hashing is implemented with the bcrypt algorithm and uses 10 salted rounds.

Multi-Factor Authentication

Midaxo Cloud supports multi-factor authentication (MFA) with Time-based One-Time Password (TOTP) to strengthen the authentication process. Customer can also enforce MFA enrolment for all users in their Midaxo Cloud account.

Breached Credential Detection

Midaxo Cloud detects and prevents the use of credentials that have been leaked through a data breach elsewhere. The breached credentials detection blocks users from logging in until the compromised password is reset.

Access Control and Authorization

Customers are logically isolated in Midaxo Cloud. For a single customer, there can be multiple processes, deals, tasks, and documents, each separated using role-based access control. Groups can be used to create fine-grained access control schemes that go beyond what roles can provide.

Each customer is granted a workspace admin account. The workspace admin is responsible for creating user accounts. Midaxo does not manage customer account credentials without a support request from the workspace admin.

Administrative Access Controls

Midaxo Cloud administrators use two-factor authentication and personal admin accounts when operating the Platform. Accounts are reviewed regularly, and passwords must meet length, complexity, and renewal requirements as defined in the Midaxo password policy.

Employee access to resources is limited to a role-based need to know basis. Access rights are granted, regularly reviewed, and deleted following the documented processes. Passwords must follow length, complexity, and renewal requirements as defined in Midaxo's password policy.

Access to the Midaxo Cloud production environment is restricted to a few software developer roles. The production environment requires two-factor authentication.

Data Security & Privacy

Data Governance

Data Residency and Location

Customers can choose to store their data exclusively in one of the Midaxo Cloud instances. Midaxo currently operates one instance in EU and one in US.

Customer data stored in the Midaxo EU instance is physically located in the AWS Ireland Region (Dublin). Customer data stored in Midaxo US instance is physically located in the AWS Ohio region. All data stored in every Midaxo Cloud instance is considered confidential.

Data Ownership and Access

Customers have ownership of their data. Midaxo's policy restricts Midaxo personnel, including admins, access to customer data to support purposes only when requested by the customer. The principle is that support is primarily conducted without accessing or seeing the customer's data and, secondarily, if necessary, by arranging a screen-sharing session or the customer granting temporary access rights to a project and data. Midaxo Cloud has technical controls in place to prevent Midaxo production administrators from accessing customer data and separate approval from Midaxo management is required for gaining access to customer data for production administrative tasks or for technical troubleshooting on support requests.

Data Release Policy

Midaxo guarantees that customer data or log files are only released if demanded by a court order. Midaxo always notifies the customer prior to any release taking place.

Data Retention and Deletion

Customer account and all other customer data associated with the account is deleted automatically from Midaxo Cloud operational systems within 30 days of account termination or expiration. Data is still stored in backups for a year. After one year, the backups are disposed by automated lifecycle policies.

Data Protection

Encryption in Transit

All end-to-end data transmissions are encrypted with 256-bit AES TLS. Transmissions between the client computer and the application use the HTTPS protocol with TLS 1.2 or newer protocol.

Encryption at Rest

Data stored in the Data Persistence layer is encrypted at rest and Amazon Key Management Service (KMS) is used for key management with 256-bit AES-GCM encryption keys. Keys are rotated annually.

Malware Detection

Midaxo Cloud scans all uploaded files for malware automatically and quarantines infected files, preventing all access to the file. Midaxo Cloud uses commercial grade anti-malware software for scanning.

Key Management

Midaxo's policy defines an information classification scheme and the acceptable use of classified information. The policy defines the use of cryptographic controls. For example, sensitive information is always transmitted in encrypted form. Cryptographic keys are stored in Amazon KMS securely outside the customer database instance.

Customer Data Isolation

Each customer's data is stored in databases that are logically isolated from other customers. Each row in the database is identified with customer's universally unique identifier (UUID). Same isolation by customer's UUID is used within the document storage and events published between the services.

Resource UUID	Customer UUID	...
3f9abd14-b94e-434a-a532-b22a161eb51c	7961f694-b0cb-4c51-97d9-0113b406ae0f	...
c99f5179-8dd7-4965-8a78-3eb56401c38c	7961f694-b0cb-4c51-97d9-0113b406ae0f	...
029d82fd-414f-43b8-93ba-4758b7574455	426fc032-9957-45da-a711-791cc4e11909	...

The use of access control list-based, item-level permissions provides a secondary safeguard against possible failures in data isolation between customer accounts. All stored deals, tasks, documents, etc. have item-level permissions, in addition to customer data isolation, to ensure that only authorized users can access them.

The possibility of circumventing access rights or isolation between customer accounts are analyzed and tested in each development iteration by Midaxo's own development team, and periodically by an independent external auditor.

Application Security

Secure Software Development Lifecycle

Midaxo utilizes Agile processes in software development, allowing the management of software releases from the development phase to release as an ongoing cycle of software development, testing, and release.

Midaxo Cloud is built on top of AWS managed services and is fully Serverless (Midaxo is not managing any virtual machines or physical servers).

The software architecture follows AWS' and Auth0's best practices for secure multi-tenant application design

Midaxo has defined policies and procedures for software development, testing, and release management. Development and testing are performed in an environment that is separated from the Midaxo Cloud production environment. Midaxo uses a Microsoft Visual Studio Code development environment and similar tooling, and Git for source code management.

Security Integration in Development

Information security is integrated into the requirement definition, testing, and code review phases. In the requirement definition phase, information security is always considered based on a risk analysis. Vulnerabilities are tested during the software testing phase with test automation. Midaxo holds a code review meeting as part of development sprints. Midaxo uses peer review and automated tools for static code analysis.

Security Testing

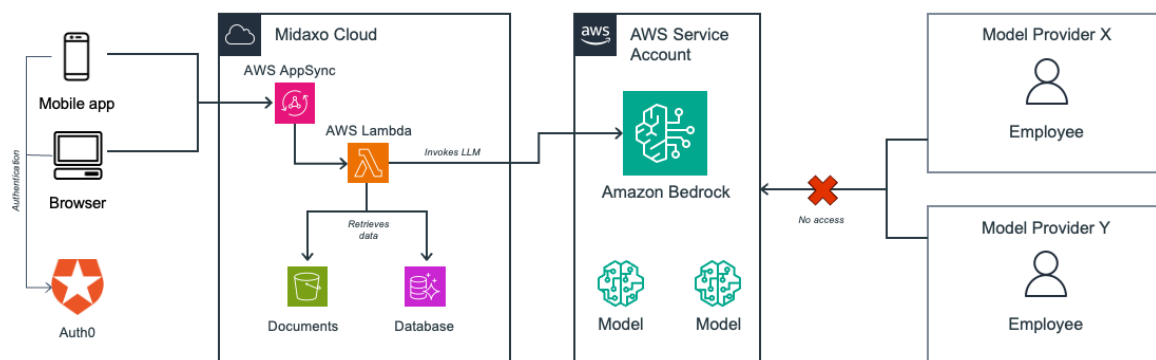
Additionally, Midaxo Cloud is continuously scanned for vulnerabilities using Dynamic Application Security Testing (DAST), Static Application Security Testing (SAST) and Software Composition Analysis (SCA) tools. In addition to internal testing, Midaxo uses independent security expertise services companies regularly to perform penetration testing on the application.

AI Security & Governance

AI Integration Architecture

API-based Integration Model

Midaxo Cloud AI is built on AWS Serverless Computing infrastructure, leveraging Amazon Bedrock for secure model access and deployment. Midaxo Cloud uses Bedrock's API to interact with the models.



No Training of Bedrock Models on Customer Data

With Amazon Bedrock Midaxo Cloud can leverage different model providers securely without exposing customers confidential data or prompts to additional parties. Customer data is not stored for the foundation model's use nor used for model training purposes.

Amazon Bedrock foundation models are deployed to AWS Model Deployment Accounts that are fully managed by AWS. Model providers do not have access to these accounts. The [Amazon Bedrock Data protection](#) page provides additional documentation.

Stateless Processing

All data passed from Midaxo Cloud to Bedrock models is only used for processing the request and data is not stored persistently in the Bedrock environment

Midaxo Cloud uses Amazon Bedrock foundation models either from AWS regions in EU or US via cross-region inference due to model availability.

AI-Specific Security Controls

Control What is Processed by AI

Customers can limit, which processes within Midaxo Cloud have AI enabled and which not. This can be used to exclude highly sensitive data from AI's processing completely.

Input Validation and Sanitization

Input validation and sanitization are implemented through Amazon Bedrock Guardrails, ensuring content safety while maintaining data confidentiality.

Output Filtering

Output filtering is implemented through Amazon Bedrock Guardrails, preventing AI's responses to contain restricted topics.

Access Management

All AI operations are subject to the same role-based access control system that protects the Midaxo Cloud platform and AI operates with the same permissions as the authenticated user.

Auditability of AI Actions

Midaxo Cloud will log additional information to its audit log, when customers perform updates to their data based on AI's suggestion. These logs will provide traceability where the AI found the information and provides a mechanism for customers to validate the correctness of the suggestion afterwards.

AI Governance

Risk Controls

Our AI implementation integrates with Midaxo's existing risk management framework while adding specific controls to mitigate AI-related risks. All risk controls are regularly reviewed and updated based on performance data and emerging threats.

Quality Assurance

Midaxo performs quality assurance validation for the AI systems to ensure that responses from the AI remain accurate through model updates and changes within the AI implementation. These tests will be maintained and extended as new capabilities are added.

Biases & Fairness

Midaxo Cloud uses Amazon Bedrock's foundation models without any fine-tuning or additional model tuning. This approach reduces the risk of bias introduced into the AI's responses, as unbalanced training data can manifest biases to the logic.

Midaxo Cloud's AI is instructed to operate fairly and without prejudice and with the default foundation models the risk of unfair responses is reduced.

Regulatory Compliance

Our AI implementation is designed to comply with the EU AI Act requirements for limited risk systems and maintains alignment with existing data protection regulations. Regular security audits are conducted to verify compliance with applicable standards and regulations. The system maintains detailed audit trails and documentation to demonstrate compliance while protecting customer confidentiality.

Intellectual Property Rights Protection

All AI-generated outputs are owned by the customer, with indemnification coverage provided through our model providers for the generated output and for the training data used for the foundation models. Customers are responsible for the content provided as input for the AI implementation.

Transparency on Model Fine-Tuning

The foundation models used can be fine-tuned in the future with corporate development and M&A specific data to provide domain-specific knowledge to the AI. Midaxo will provide detailed description of the data used for the fine-tuning process. Customer data will not be used for fine-tuning models that would be shared across customers.

Threat Detection & Monitoring

Security Operations Monitoring

Infrastructure and Application Monitoring

Midaxo monitors continuously for alarms generated by various automatic monitoring systems. Midaxo Cloud's availability is monitored by an automated service with heartbeat functionality, ensuring that both front-end and back-end services are available and responding correctly.

Security Event Monitoring

The platform security is monitored in real time for threats and misconfigurations. Alarms generated by the SIEM solution are analyzed and escalated to Midaxo's incident management process to ensure proper incident response.

Login Attempts and Access Events

Login attempts to Midaxo Cloud are monitored to detect malicious attacks such as brute-force attacks on a customer's account. The number of allowed incorrect credential combinations is restricted, and abnormal activity is reported to the affected customer.

Midaxo Cloud application usage and access management events are logged, which allows Midaxo support to manually investigate potential cases of misuse reported by customers. Midaxo's access to the application log files is limited to named personnel.

Customers can use the built-in Midaxo Cloud audit log to view detailed actions taken within their Midaxo Cloud processes.

Vulnerability Management

Midaxo maintains a list of all third-party components used in Midaxo Cloud and automated systems follow published vulnerabilities and software updates related to the third-party components.

In addition, Midaxo closely monitors security updates, alerts, and advisories from various security organizations and authorities to monitor security threats and possible vulnerabilities. Based on risk analysis results, Midaxo deploys applicable mitigation methods and security controls when required.

Incident Response & Business Continuity

Incident Management

Detection and Reporting

Midaxo's policy holds each employee responsible for reporting perceived security incidents. Midaxo Cloud customers can report incidents by contacting customer support.

Midaxo also receives alarms via various automatic channels. Alarms are investigated to determine if it is an incident.

All reported incidents are logged with remedial actions indicated. Critical security incidents and data breaches are always promptly reported to the affected customers upon discovery. Each incident will be analyzed to determine whether changes in the existing architecture or implementation are necessary.

Customer Notification

In case of a data breach or any other critical security incident, Midaxo always notifies the affected customers immediately upon discovery and informs them of the scope and mitigation activities. To date, Midaxo has never experienced any data breach incidents.

Business Continuity Measures

Backup Strategy

Midaxo Cloud data is automatically backed up daily. All backups are encrypted with Amazon Key Management Service (KMS). The daily backups are stored for 90 days, and monthly backups are kept for one year. Restoration tests are performed quarterly to ensure their successful execution.

High-Availability with AWS Availability Zones

All customer data can be fully recovered in case of hardware failure or an outage of the Amazon service. Midaxo Cloud runs on multiple AWS availability zones and outages in a single availability zone do not affect the service availability.

Disaster Recovery

Midaxo Cloud's disaster recovery (DR) plan is exercised once per year to ensure the capability to rebuild the full system from scratch and restore service within the RPO of 24 hours.

Service Status Communication

Information about Midaxo Cloud outages will be published on the Midaxo Cloud status page at <https://status.midaxo.com>.

Physical & Environmental Security

AWS Data Centers

AWS deploys comprehensive physical security measures to protect its data centers. To maintain certifications such as ISO/IEC 27001 Information Security Management, AWS is required to set up and maintain physical security controls such as video surveillance, physical access management, visitor access rules, and protection against exterior threats such as burglary or fire.

For more information about the physical security of AWS data centers, visit the [AWS Security Center](#).

Midaxo Offices

Midaxo's offices are protected with the following physical security controls:

Physical Access

Physical access to Midaxo's offices is granted to authorized personnel only. Access rights are reviewed regularly.

Visitor Access

Visitor access rules restrict visitor access to limited areas. All visitors are registered and escorted by Midaxo personnel.

Protection Against External Threats

Midaxo's offices are protected with 24/7 video surveillance as well as intrusion and fire alarm systems.

Data Storage


Midaxo Cloud production data and customer data are not stored on Midaxo office premises. Primary copies of software source code and other operation-critical data are stored off-site to ensure disaster recovery capabilities in crisis situations.

Change & Release Management

Change Management Process

All changes to Midaxo Cloud and software are processed in accordance with the Midaxo change management process. The change management process ensures that all changes are properly planned, approved, and documented, and that associated risks are analyzed, and changes are implemented in a controlled manner.

Software Development Process



Midaxo utilizes Agile processes in software development, allowing the management of software releases from the development phase to release as an ongoing cycle of software development, testing, and release. Midaxo has defined policies and procedures for software development, testing, and release management. Development and testing are performed in an environment that is separated from the Midaxo Cloud production environment.

Version Control and Release Authorization

Decision-making points are set to determine software versioning and the version to be released. Engineering personnel only have access to the software code repository and are authorized to make release decisions.

Third-Party Risk Management

Supplier Selection and Management

Midaxo chooses suppliers carefully following a defined set of criteria. Supplier access to information is limited on a need-to-know basis, depending on the supplier's role and assigned responsibilities. Non-disclosure agreements are signed with suppliers.

Third-Party Component Management

Midaxo uses only well-known services or third-party libraries for product development and for delivering Midaxo Cloud. Midaxo maintains a list of all third-party components in use and regularly follows published vulnerabilities and software updates related to the third-party components.

Asset Management

Midaxo manages an inventory of assets, and the acceptable use of assets is defined in the respective policies. Midaxo uses an information classification scheme to ensure that information is appropriately protected. Classified information is labeled and handled according to each classification. When assets, both electronic and paper, are no longer needed, disposal is handled securely according to formal procedures.

Human Resources Security

Human resources ensure information security within processes for new personnel recruitment, during employment, and on termination of employment. For example, during recruitment, candidates are interviewed and background-checked (when permitted by legislation), each new employee's induction includes Midaxo information security training, and information security awareness is maintained by regular training during employment.

Disclaimer, Trademark and Copyright Notices

Disclaimer

This documentation is provided "as is" and all express or implied conditions, representations and warranties, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement, are disclaimed, except to the extent that such disclaimers are not enforceable by law. Midaxo shall not be held responsible, under any circumstances, for any indirect damage, including, but not limited to, any incidental or consequential loss (including monetary losses), that might result from the use of this documentation, or the information disclosed in it. Information in this document is subject to change without prior notice.

Trademarks

The Midaxo name and the Midaxo logo are trademarks of Midaxo Oy. Midaxo M&A Platform is a trademark of Midaxo Oy. All third-party trademarks are the property of their respective owners.

Copyright

The copyright of this document is vested in Midaxo Oy. No part of this document may be reproduced, translated or transmitted in any form or by any means, electronic or mechanical, for any purpose without the express written permission of Midaxo Oy, and then only on the condition that this notice is included in any such reproduction.