Midaxo

Midaxo Security Whitepaper

Version 2018-08

Classification: Public

Executive Summary

Midaxo is committed to maintaining a high level of information security, and its key priority is always protecting customers' information and carefully maintaining the information security of Midaxo Platform. This Security White Paper gives an overview of the Midaxo Platform security features.

The certified Midaxo information security management system (Midaxo ISMS) complies with the international ISO/IEC 27001:2013 standard. The design of security controls is based on risk analysis. Risk management is periodically performed throughout the organization to ensure the mitigation of any emerging security risks. Midaxo ISMS defines the security processes, roles, and responsibilities for implementing information security management as an integral part of Midaxo's business and operations. Midaxo ISMS, together with Midaxo's information security policy, are periodically reviewed to ensure they are up to date.

Midaxo Platform is developed, operated, and maintained by motivated, competent personnel that are committed to maintaining a high level of information security. Continuous security education and training supports them to maintain security awareness in the organization. The technical implementation of Midaxo Platform has been designed to meet customers' strict security requirements and industry best practices.

Technical security starts with comprehensive security architecture that defines a solid and secure foundation for Midaxo Platform. The architecture is based on well-proven and widely used secure products, methods, and protocols, and it has been defined to protect data both in transit and at rest and to ensure its confidentiality, integrity, and availability. Strict access control allows only authorized users to access the data.

Operation and maintenance of the Platform follows documented processes and plans. Continuous monitoring of information security and system performance ensures that all deviations and incidents can be responded to in a timely manner by trained and competent personnel in accordance with the incident response process.

Because of today's ever-changing risks and security threats, Midaxo's security team closely monitors security updates, alerts, and advisories from applicable system and software vendors as well as various security organizations and authorities. Based on risk analysis, the security team deploys applicable mitigation methods and security controls. Periodic security audits and technical tests performed by independent third-party information security companies ensure that information security fulfills all requirements and meets the highest standards.

Table of Contents

Introduction to Midaxo Platform

Midaxo Platform helps mergers and acquisitions (M&A) professionals to define and execute a systematic M&A process. The Platform can be used for many kinds of deal-making processes such as divestments, restructurings, and litigations, run in parallel.

Midaxo provides an enterprise-wide pipeline of M&A deals in different stages. Each deal has its own workspace where all deal-specific information can be stored. Deal-specific information can include workflows, tasks, documents, communication, issues, and so on.

The Platform is designed for managing confidential information such as information under stock market insider trading legislation. Therefore, it has multi-level access rights management capabilities, and, by default, users cannot view any deals. Administrative users can grant access to individual deals. In addition, within deals, administrative users have granular permissions management options to grant individual users access only to individual tasks and documents.

Midaxo Platform Architecture

Midaxo Platform runs on Amazon's leading cloud platform, the Amazon Elastic Compute Cloud (AWS EC2) Web service.

Midaxo Platform is logically based on a three-tier client server architecture, in which the user interface (presentation tier), application processing (logic tier), and data storage (data tier) functions are separated.

The Midaxo Platform production environment contains three distinct servers:

1. M&A application server

   Provides the user interface and processes the M&A software

2. M&A database server

   Provides M&A data storage, separated from the application

3. Log collection server

   Collects log data from both aforementioned servers; the server automatically sends alerts regarding any detected violations.

Software

Midaxo Platform is built on top of Microsoft technologies, including ASP.NET, SharePoint Foundation, and SQL Server. The software runs on the M&A application server with Windows Server 2012 R2 64-bit. The M&A database server utilizes Microsoft SQL Server 2014.

The software architecture follows Microsoft's best practices for secure multi-tenant application design. An SQL database, through SharePoint Foundation, is used to store customer data. The software architecture is shown in the figure below.

Midaxo uses only well-known services or third-party libraries for product development and for delivering Midaxo Platform. 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.

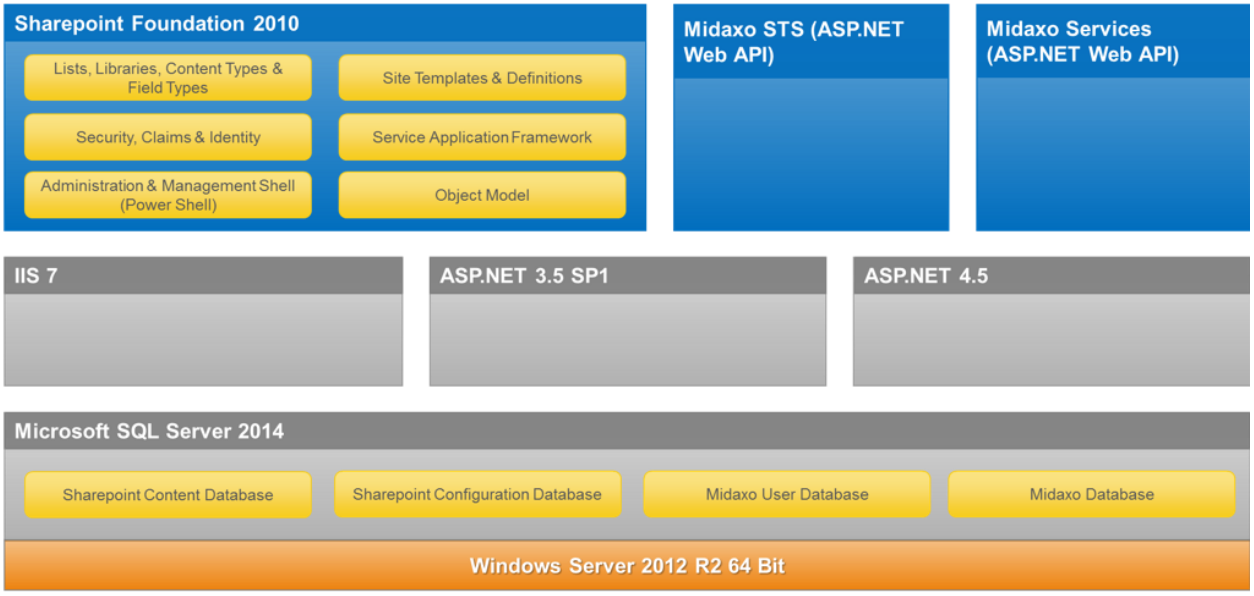

Figure 1 Software Architecture

Network Security

Midaxo Platform has industry-standard protection techniques deployed, including firewalls, network security monitoring, and intrusion detection solutions.

Midaxo Platform is accessible via a browser. All communication between Midaxo's servers and client computers is encrypted with 256-bit AES TLS certified by Network Solutions CA.

Network Segregation

The Midaxo Platform production environment contains three network segments, separated by firewalls, as shown in the figure below.

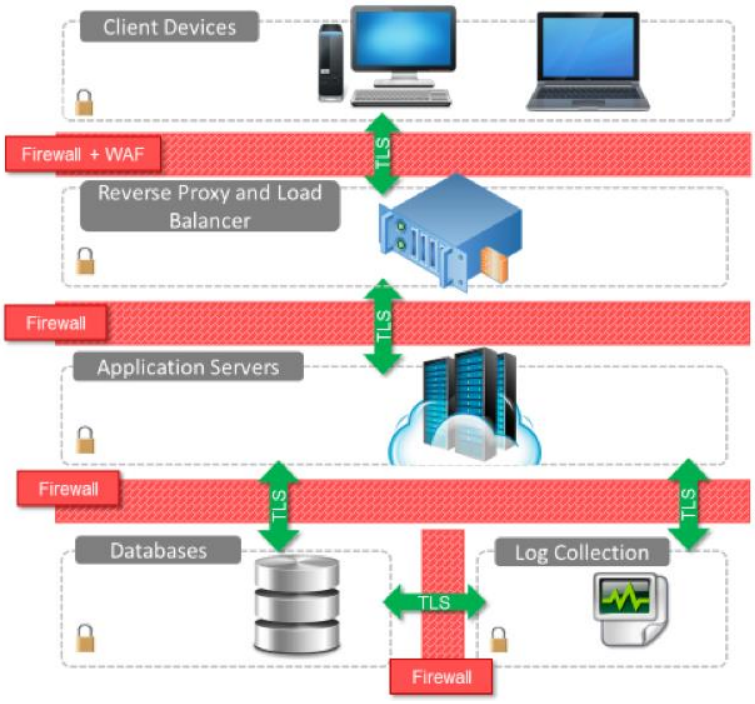

Figure 2 Midaxo Platform Network Segments

Continuous network monitoring allows comprehensive awareness of network events on a 24/7 basis. For more information about monitoring, see the Monitoring and Logging section of this White Paper.

To ensure network security, the Midaxo office network that is used for administrative work is segregated from the Midaxo Platform production environment.

Separate quality assurance and staging environments are used for testing. These environments are separated from the production environment.

Midaxo Platform Security

Midaxo Platform is built on top of Microsoft technologies such as SharePoint and SQL Server. Microsoft products are developed based on the Trustworthy Computing program. The following Microsoft products in Midaxo Platform have been Common Criteria security certified:

- Windows Server 2012 R2
- Database Engine of Microsoft SQL Server 2014

Midaxo Platform has a three-tier architecture, where data are separated from the front end and the application with separate servers for the M&A application and the database.

The Midaxo Platform servers have been security hardened with Microsoft Baseline Security Analyzer to enhance security. Independent third parties regularly audit platform security. Midaxo Platform servers are updated frequently with the latest security and functionality patches.

Midaxo Platform 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. In addition, Midaxo administrator accounts are prohibited from using the most recent passwords.

Amazon EC2 platform security is proven by the following certifications and audits:

- SOC 1/ISAE 3402
- SOC 2
- SOC 3
- Cloud Security Alliance (CSA) STAR registrant, and has completed the CSA Consensus Assessments Initiative Questionnaire (CAIQ)
- PCI DSS Level 1 compliance
- ISO 27001 Information Security Management – certification
- ISO 9001 Quality Management – certification

For more information about Amazon cloud platform security, visit the AWS Security Center.

Midaxo Platform Application Security

Authentication

To access Midaxo Platform, users are authenticated with usernames and passwords. Authenticated users get a security token to identify them. In each request to the Midaxo M&A application server, the security token is checked. Based on the security token, a user can be authorized. Midaxo platform supports two-factor authentication (TFA).

Midaxo Platform locks a user account after a defined number of failed login attempts. If a session is idle for a defined period, it will expire automatically and require the user to log in again. Customers can configure their own password policy in the Midaxo application including password length, complexity, expiration and history requirements.

Access Control

Customers are logically isolated in Midaxo Platform. For a single customer, there can be multiple processes, projects, and documents, each separated using role-based access control, as illustrated in the figure below.

Midaxo Platform has requirements for end-user password length and complexity. Passwords are hashed and then stored in the database. Hashing is implemented with the combination of HMACSHA256 and a password-based key derivation functionality PBKDF2. Hashing includes random salt and multiple iterations.

Each customer is granted one company admin account. The account admin is responsible for creating user accounts for an organization via self-service as well as with support. Midaxo does not manage customer account credentials. Company admin password recovery is performed via self-service with a two-factor authentication method. The customer is responsible for cancelling an admin account.

Besides the company admin role, three other role options are available for setting up appropriate access rights and permissions within each organization: Process Admin, Project Admin/Project Creator, and Project Member. A project admin grants access rights to project members and

administers the respective projects. Project members can only access projects or only limited sections within a project that they have been granted access rights to.

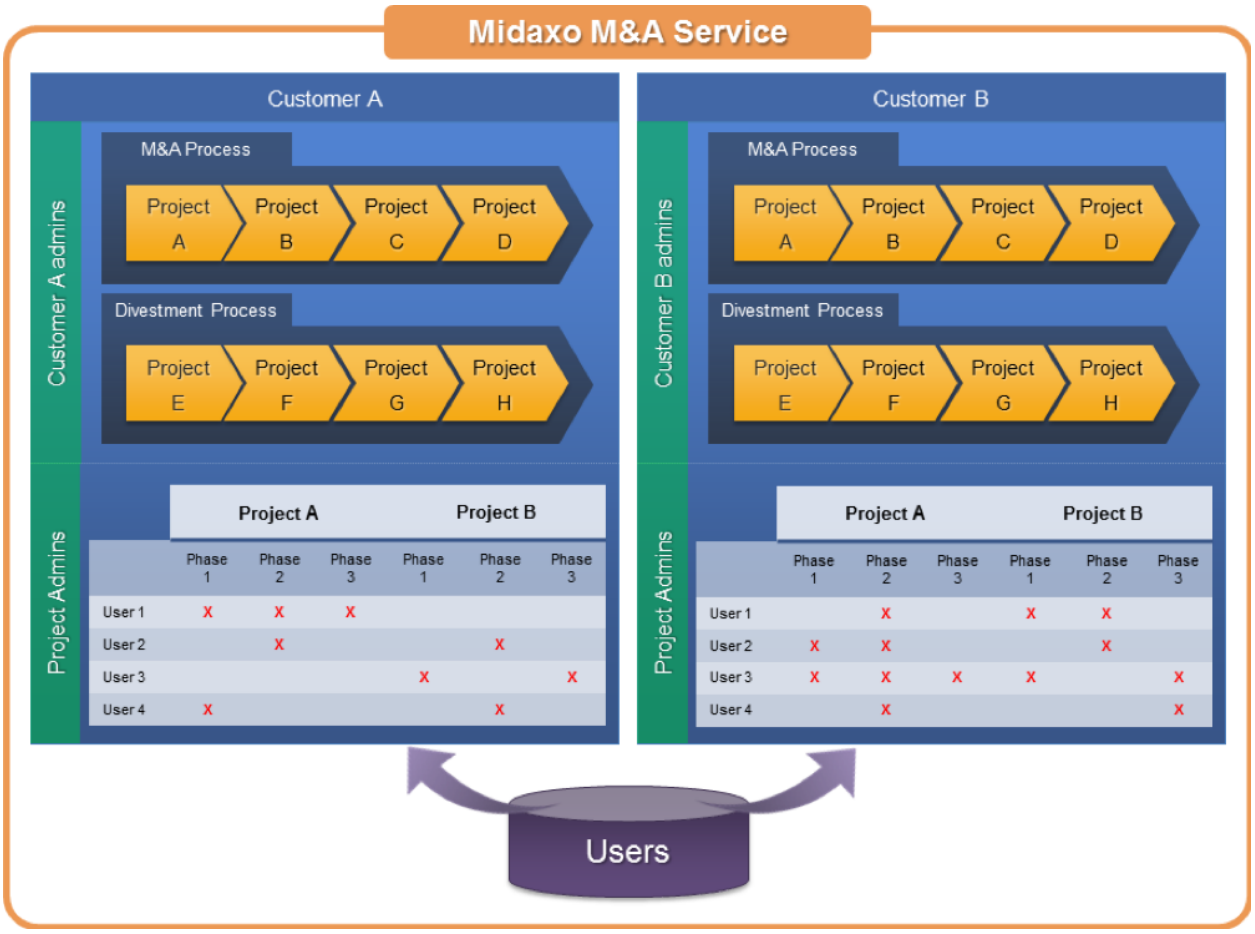

Figure 3 Midaxo Platform Access Control

Customer Data Security

Customers can choose to store their data exclusively in the Midaxo EU instance or in the Midaxo US instance. Customer data stored in the Midaxo EU instance is physically located in the Amazon EC2 Ireland datacenter. Customer data stored in Midaxo US instance is physically located in the Amazon EC2 North Virginia datacenter. All data stored in every Midaxo Platform is considered confidential.

Customers have ownership of their data. Midaxo policy restricts Midaxo admin's 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.

Customer account and all other customer data associated with the account are deleted automatically from Midaxo Platform within 60 days of account termination or expiration. Data are still stored in daily backups, off-site backups, and VM hard-disk snapshots for a year. After one year, the customer data are deleted completely in accordance with Amazon AWS's policy. Customers can also download all their data as file exports from the Platform.

Data Security in Transit and at Rest

All end-to-end data transmissions are encrypted with 256-bit AES TLS. Transmissions between the client computer and the M&A application server use the HTTPS protocol with TLS. In addition, transmissions between the M&A application server and the database server are encrypted. SQL Server Enterprise edition is used as the database engine. Transparent Data Encryption, provided by SQL Server, is used to encrypt the stored data. Midaxo follows Microsoft's architecture recommendations, as well as expert advice by security advisors, for building a secure multi-tenant architecture.

Each customer's data are stored in databases that are logically isolated from other customers. Each row in the database is identified with customer's globally unique identifier as shown in the figure 4.

Guid	Customer Guid	…
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	…

Figure 4 Midaxo M&A Customer Data Separation

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 projects, 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.

Data breach notification practices

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.

Data Release

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.

Monitoring and Logging

Midaxo's monitoring team is always on standby for alarms generated by various automatic monitoring systems.

Midaxo Platform's availability is monitored by an automated service with heartbeat functionality, ensuring that both front-end and back-end servers are available and responding correctly. Amazon provides automated monitoring for server resources, such as CPU, memory, and storage capacity.

The network is monitored 24/7 with intrusion detection solutions and firewalls. Alarms generated by intrusion detection and firewalls are analyzed and escalated in a timely manner to Midaxo's incident management process to ensure proper incident response.

Midaxo monitors login attempts to Midaxo Platform 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 Platform 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 strictly limited to admin personnel, and Midaxo's policy only allows access for support purposes.

Furthermore, Midaxo Platform system logs are monitored to detect any abnormal activity.

Midaxo Platform Availability and Continuity

Backups and Redundancy

Midaxo Platform servers and all customer data are automatically backed up on a daily basis. Backups are stored at a separate off-site location in Frankfurt, Germany for Midaxo EU instance, and in Ohio for Midaxo US instance. All off-site files are encrypted with AES-256. The daily backups are stored for 90 days, and monthly backups are kept for one year.

All customer data can be fully recovered in case of hardware failure or an outage of the Amazon service. Midaxo Platform can be moved to another Amazon availability zone in case of outages with the latest snapshot. If a customer deletes data by accident, prompt contact to Midaxo support ensures successful data restoration, as the Platform offers features to prevent accidental permanent deletion of files.

Continuity and Disaster Recovery

Midaxo's business continuity plan covers various scenarios with prevention, response, and recovery strategies. The continuity plan is regularly updated based on a risk analysis, and Midaxo's monitoring team regularly tests the plans and work instructions.

Information about Midaxo Platform outages will be published on the Midaxo website, and affected customers will be notified immediately upon discovery.

For details on Amazon Web service availability and disaster recovery, visit the following Web pages: http://aws.amazon.com/architecture/ and http://aws.amazon.com/backup-recovery/.

Physical Security

Amazon Data Centers

Amazon deploys comprehensive physical security measures to protect its data centers. To maintain certifications such as ISO/IEC 27001 Information Security Management, Amazon 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 Amazon 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.
- Badges: Midaxo personnel are required to wear badges at the Midaxo offices at all times. Badges are regularly renewed.
- 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.

Midaxo Platform 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.

Midaxo's 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 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 current status. The management team acts as an information security steering group. Midaxo's chief technology officer is responsible for information security management.

Processes

Midaxo has defined a set of processes to ensure information security in all of its operations as well as in Midaxo Platform.

Software Development, Testing, and Release

Midaxo utilizes the Kanban method 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 Platform production environment. Midaxo uses a Microsoft Visual Studio development environment, and Git for source code management.

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 at the end of every development sprint. Midaxo uses peer review and other tools for static code analysis. Additionally, Midaxo platform is continuously scanned for vulnerabilities using Dynamic Application Security Testing (DAST) tools.

Decision-making points are set to determine software versioning and the version to be released. Only a strictly limited number of development personnel have access to the software code repository or are authorized to make release decisions.

The skills and awareness of Midaxo's software developers are continuously enhanced with OWASP top 10 vulnerabilities, for example, and information security training provided by third parties such as Microsoft.

Vulnerability Management

Regarding vulnerability management, Midaxo maintains a list of all third-party components used in Midaxo Platform and regularly follows 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.

Change Management

All changes to Midaxo Platform 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.

Incident Management

Midaxo's customers can report incidents through the feedback function or by contacting customer support. Midaxo's policy holds each employee responsible for reporting perceived security incidents. Midaxo also receives alarms via various automatic channels. These are discussed in greater detail in the Monitoring and Logging section of this White Paper. Each alarm will be escalated as quickly as possible. Each incident will be analyzed to determine whether changes in the existing architecture or implementation are necessary. All reported incidents are logged and the remedial action indicated. Critical security incidents and data breaches are always promptly reported to the affected customers upon discovery.

Access Control

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 software code repository and the Midaxo Platform production environment is restricted to a few software developer roles. The production environment requires two-factor authentication.

Other Processes

1. Risk management

   Internal and external risk analysis is performed regularly. Identified risks are managed with prevention, mitigation, response, and recovery strategies. Policies and processes are continuously improved based on the risk analysis findings.

2. Human resources

   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, each new employee's induction includes Midaxo information security training, and information security awareness is maintained by regular training during employment.

3. Asset management

Midaxo manages an inventory of assets, and the acceptable use of assets is defined in the respective policies governing teleworking and mobile usage. 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.

4. Supplier 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.

5. 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 a separate Hardware Security Module (HSM) outside customer database instance.

Certifications & Audits

Midaxo has ISO/IEC 27001:2013 Information Security Management certification. ISO 27001 is an internationally recognized security management standard that specifies security management best practices and comprehensive security controls.

The Midaxo Platform service has an Information Security Certificate issued by Nixu Ltd., the largest independent information security expert services company in the Nordics. The Information Security Certificate verifies that the Midaxo Platform architecture and software are designed, implemented, and maintained securely. Nixu Ltd. performs an annual security audit to maintain the Nixu Information Security Certificate. Besides Nixu Ltd., other independent third-party auditors regularly audit Midaxo Platform's security.

In addition, customers have audited Midaxo Platform. Midaxo offers customers the opportunity to perform security audits and penetration testing of their own with a test instance with the same architecture as in Midaxo Platform.

Personal Data

Midaxo's practices for collecting, processing, protecting, and disclosing personal data are detailed in Midaxo's Privacy Policy.

The following personal data are processed and stored in Midaxo Platform during the registration process:

1. First and last name
2. Company address
3. Work phone number
4. Work email address

All customer data are stored in the Amazon cloud service. Main location of the data is Ireland (Dublin) and backup location Germany (Frankfurt) in EU, and North Virginia and backup location Ohio in US.

For additional information on compliance provided by Amazon Web Services, see http://aws.amazon.com/compliance.

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 Ltd. Midaxo M&A Platform is a trademark of Midaxo Ltd. All third-party trademarks are the property of their respective owners.