
NOMENTIA
WHITEPAPER
Security at
Nomentia

Table of Content

Introduction

The mission of Nomentia is to provide its customers with unparalleled solutions for cash and treasury management.

Making your data secure and protecting it is one of our most important responsibilities.

Nomentia is committed to being transparent about its security practices and helping you understand our approach.

Information Security Policy

Nomentia's security program is based on the concept of defense in depth; securing our organization and your data at every layer. Our Information Security Management System is, according to the ISO/IEC 27001:2013 standard, constantly evolving with updated guidance and new industry best practices. You can see all our information security certificates here.

ISAE 3402
CERTIFIED TYPE II

FSQS-NL
REGISTERED

SWIFT Compatible Application

ISO ISO/IEC 27001:2013

Certifications

ISO/IEC 27001:2013 ISMS

ISO/IEC 27001 is the standard used to define the Information Security Management System (ISMS).

Nomentia operates according to its certified ISO/IEC 27001:2013 Information Security Management System (ISMS). The scope of the ISMS includes the people, information systems, processes, and services provided by Nomentia cash and treasury management solutions, including all corporate functions and premises.

The ISMS defines the purpose, principles, direction, and basic rules for information security management at Nomentia.

ISAE 3402 Type 2

International Standard on Assurance Engagements 3402 (ISAE 3402), titled Assurance Reports on Controls at a Service Organization, is an international assurance standard that prescribes Service Organization Control (SOC) reports.

The Nomentia Cash Management service is audited according to the ISAE 3402 Type 2 controls, and the annual assurance report is made available for Nomentia's customers who use the service.

SWIFT Customer Security Program

The SWIFT Customer Security Program (CSP) is intended to actively support customers in the fight against cyber-attacks.

The CSP program is a mandatory certification program for SWIFT partners, such as Nomentia. It enhances SWIFT-related tools for customers and provides a set of cybersecurity controls that help users strengthen end-point security and combat cyber fraud.

The Nomentia Cash Management service is audited according to the SWIFT CSP controls, and the list of certified SWIFT partners can be found at https://www.swift.com/about-us/partner-programme/lite2-business-application-providers-directory.

FSQS-NL Supplier Qualification System

The FSQS-NL Registered Mark is valued by some of the largest purchasers in the financial sector and indicates that the organisation has gone through the process required to demonstrate its commitment and credentials to the industry.

Information Security Governance

Information Security Governance Framework

Internal control, enterprise risk management, code of conduct, environmental and social governance, and Nomentia's values are essential parts of the corporate governance of Nomentia. Work and practices in Nomentia follow documented processes and procedures.

Roles & Responsibilities for Information Security

The Nomentia security team, led by the Chief Information Security Officer (CISO), is responsible for the implementation and management of our Information Security Management System and the security governance framework.

Personnel Security

Employee Security

Background verification checks on all candidates for employment are carried out in accordance with relevant laws, regulations and ethics. Nomentia performs the screening of candidates, and classified personally identifiable information is accessed only by human resources personnel. Employees who operate with the cash management cloud services are screened, and the vetting is periodically renewed every five years.

Training & Awareness

Employees of Nomentia receive security and privacy awareness training both as part of their onboarding process and as an annual refresher. The security awareness training covers, but is not limited, to the following topics:

- General information security requirements
- Phishing awareness and prevention
- Clean desk policy & teleworking policy
- Password policy and management
- Security incident management
- Office physical security
- Labeling of information
- Data privacy
- Secure development guidelines and OWASP principles
- Secure operations and change management
- SWIFT Customer Security Program requirements

Information Security Policies and Controls

Access Control

Nomentia has a formal access control policy that defines access to Nomentia assets.

- Access to all computing systems is restricted to authenticated accounts and authorized users only.
- Authorization to computing systems is granted on a need-only basis, with the least privilege principle.
- Access to services is only allowed using end-to-end encrypted and authenticated connections.
- All services and environments are protected with strong authentication. This may mean certificates, multi-factor authentication, biometrics, or other forms or combinations of authentication that are generally considered strong. Single-sign-on and multi-factor authentication is used for personal accounts.
- Access to customer confidential or sensitive information – including but not limited to customer content and Personally Identifiable Information – is prohibited for a purpose other than as legally required and to operate the services unless access to the information is specifically allowed by the customer.
- Access to computing systems is monitored based on the audit records generated and stored in the SIEM system.
- All systems (application, databases, and operating systems) are hardened to enforce information security policy requirements for password administration.
- All user accounts are reviewed periodically to ensure that malicious, out-of-date, or unknown accounts do not exist.

Acceptable Use of Assets

The Nomentia acceptable use of assets policy defines the requirements for how employees safeguard internal or confidential information when using or having access to the organization's assets.

The policy includes, but is not limited to:

- Classification and labeling of information
- Handling of assets
- Management of removable media
- Disposal of media or equipment
- Physical media transfer
- Regulation of cryptographic controls and key management
- Equipment maintenance and security on and off-site
- Removal of assets
- Unattended equipment, clear desk, and clear screen policies
- Controls against malware
- Restrictions on software installation
- Information transfer policies and procedures
- Agreements on information security
- Electronic messaging
- Confidentiality or non-disclosure agreements
- Intellectual property rights

Logical access to Nomentia provided services

Nomentia's cloud services are used with a web browser, where customer end-users log into the service using a secure internet connection (https) and personal login credentials. Authentication can be done using Single-Sign-On federation and Multi-Factor Authentication.

Access to the services is role-based and the customer has control over end-user management and user permissions. Nomentia does not operate the services on behalf of the customer.

Physical Security

Only Nomentia employees or external personnel under contract have access to Nomentia premises.

To identify employees, Nomentia employees wear the employee photo-ID badge while at the office or working at customer premises.

All visitors accessing the Nomentia offices are registered and are required to have a host accompanying them for the duration of the stay.

Network Security

Nomentia cloud services are operated in protected network environments, including firewalls providing stateful packet inspection, advanced filtering features, and a Web Application Firewall (WAF) that protects from advanced threats.

To exchange files and data between the service and the customer back-end systems, Nomentia hosts a Secure File Transfer Service (SFTP) as the standard integration option. Nomentia may also offer integration for certain solutions via Application Programming Interfaces (API) and enable the customer to sign and encrypt payment files with PGP encryption.

Secure Development, Operations, and Change Management Policies

Nomentia's secure development policy provides assurance that a systematic approach is taken to software development and new applications and changes to existing applications are appropriately authorized, tested, approved, properly implemented, and documented.

The secure change management policy provides assurance that changes and updates to existing system software and cloud infrastructure are authorized, tested, approved, properly implemented, and documented.

The operations policy provides assurance that performance and availability of adequate technical resources are continuously monitored, and automated alerts are implemented to detect and warn impending resource shortages.

Development and testing environments are separated from operational environments. Operational data containing personally identifiable information, customer data or any other confidential information is not used for development or testing purposes.

Static Code Analysis

Static code analysis tools and integrated vulnerability scanners are used as a part of the development process to prevent the deployment of potentially insecure code and vulnerabilities to the Nomentia-provided services.

Vulnerability Scanning

Nomentia performs regular vulnerability scanning on its cloud platforms. Reported vulnerabilities are treated according to the Nomentia risk and change management policy.

In addition, vulnerability scanning is part of the Nomentia software release model. Vulnerability scanning is conducted on each release candidate and the results are analyzed. The go/no-go decision for the release deployment is based on the outcome of the analysis.

Penetration Testing

Regular internal and external penetration testing is performed to identify potential security weaknesses on cloud platforms, networks and software. The testing procedures and results are audited annually as part of the Nomentia certification audits.

Audit Logs

Audit logs from Nomentia provided cloud services, employee end-points, and office networks are collected and stored in immutable form to the Nomentia Security Information & Event Management (SIEM) system, and monitored 24/7 by the Nomentia Security Operations Center (SOC) for signs of information security incidents.

Logs are stored according to the internal log retention policies, and access is restricted to authorized personnel only. The audit trail is always available for the latest actions in the service, and the log data can be used as forensic evidence for information security incident resolving.

Solution related logs can be viewed by customer end-users within the Nomentia service, according to their user permissions of the solution. The solution logs provide audit trail information regarding the customer's service usage, such as access log, change log and action log.

Anti-virus & anti-malware

Anti-virus and anti-malware software is used on all end-point devices and servers.

Email security

Corporate email is scanned in the email gateway before delivery to the inbox. Suspicious or malicious content is filtered or quarantined by the email service prior to delivery to the inbox. Nomentia uses email encryption for sending confidential information to external recipients.

Incident Response

The Nomentia Information Security Incident Management policy ensures a consistent and effective approach to the management of Information Security Incidents, including communication on security events and weaknesses.

The policy provides a definition of an Information Security Incident and establishes a structure for the reporting and management of such incidents.

The Nomentia Information Security Incident Response Plan, coordinated by the Nomentia CISO, provides direction and focus for handling information security incidents. The purpose of the plan is to coordinate a quick and appropriate response to information security incidents.

Security incidents are managed by the Nomentia Cyber Security Incident Management team (CSIMT) and Cyber Security Incident Response Team (CSIRT).

Data Privacy

The Nomentia Privacy Policy can be read here. Also, please see the Nomentia General Terms and conditions, data processing agreement, and list of technical and organisational security measures for additional information on data privacy and the processing and securing of customer data.

Nomentia's Data Privacy Officer is responsible for assessing and managing data privacy together with the Nomentia legal and security teams.

Data encryption

Data is encrypted in transit and at rest: user sessions via HTTPS/TLS 1.2 and integration services via SFTP. In addition, PGP can be used to encrypt and digitally sign payment materials with certain services. Database connections are encrypted with TLS 1.2, databases, and database backups with AES-256. Encryption keys used to encrypt data are stored and managed by Nomentia.

Data isolation is implemented on a database level.

Data Processing Locations

Customer data is stored and processed within the European Union/European Economic Area.

Data Retention in Nomentia Services

The retention period of the customer data stored in Nomentia-provided cloud services is two years by default but can be extended up to ten years depending on the service level agreement and the options purchased by the customer.

Access to Customer Data

Nomentia provides its services to its customers according to its general terms and data processing agreement, available at https://cash.nomentia.com/general-terms. The data processing agreement sets out the terms and conditions for the processing of personal data by Nomentia, on behalf of the customer.

Nomentia as the service provider provides the end customer with a master user account at the beginning of the cloud service implementation. The customer is responsible for creating and managing the necessary user accounts for the end-users of their own organization. Each Nomentia cloud service end-user is provided with an individual username in the user administration of the service.

Nomentia may use a service desk account to log into the customer system to help troubleshoot service-related customer inquiries that arise from the customer's end-users. The customer is responsible for managing the permissions of such an account and may deny or grant access to such an account of their will. By default, Nomentia does not have access to the user administration of the customer's cloud service.

Returning of Customer Data at Subscription Termination

Nomentia will securely destroy any customer data in its possession after one (1) month following the termination of the service agreement.

Upon the customer's request and in exchange for reasonable compensation, Nomentia will provide reasonable assistance to the customer in issues relating to the customer stopping using the Service and to help return all customer data stored in the cloud service.

Subcontractors

Nomentia uses subcontracting to provide its cloud services or services related to them. The customer enters into an agreement only with Nomentia and Nomentia remains liable for the work, acts, and omissions of its subcontractors.

The list of Nomentia subcontractors, including the scope, purpose, and location of data processing, is available at https://cash.nomentia.com/general-terms.

Responding to requests under data subjects right

To respond to requests from data subjects exercising their rights, such as the right of access and the right to rectification or erasure, Customers need to primarily use the corresponding functions of the cloud services. Where this is not possible by the Customer's user privileges in the cloud services, Nomentia shall provide its Customers with commercially reasonable assistance, taking into account the nature of the processing.

Disaster Recovery & Business Continuity

Nomentia Cloud Services are secured using the principle of High Availability with primary and secondary hosting locations. This means that when one component breaks or its functioning is interrupted, another similar component continues to function.

In the event of the unavailability of a single data center, there would be no production service disruption. In the event of data loss, data would be restored from offline backup storage with the RPO and RTO defined in the service level agreement for the applicable cloud service.

Offline backups are stored in a separate location from the operational environment and encrypted at rest.

Disaster recovery and business continuity are managed according to the Information Security Management System. Nomentia conducts annual business continuity and disaster recovery tests to determine that the appropriate controls are in place.

Business continuity and disaster recovery management are audited by external auditors as part of the ISO/IEC 27001:2013, ISAE 3402 Type 2 and SWIFT Customer Security Program audits.

Conclusion

We have an existential interest in protecting your data. Every customer and organization deserve and expect their data to be secure and confidential. Safeguarding this data is a critical responsibility we have to our customers, and we continue to work hard to maintain that trust. Please contact your Nomentia representative if you have any questions or concerns regarding our security measures.


NOMENTIA