NewBanking

Security Whitepaper

Revision History

Version	Date	Revision Author(s)	Summary of Changes
1.0	25-Nov-2020	Anders Boberg (Zacco) Morten Helles	First version.
1.1	10-Sep-2021	Morten Helles	Minor changes as part of yearly review.

Distribution

Name	Title

Approval

Name	Position	Signature	Date
Morten Helles	CTO		10-Sep-2021

Document Classification	General information
Document Owner	CISO

Contents

Introduction

This whitepaper outlines NewBanking's approach to security for our platform, and focuses on security including details on organizational, procedural and technical controls regarding how the data you entrusted us with are protected, managed and used.

Security is Part of our DNA

Employee Background Checks

As part of our recruitment process, NewBanking will verify the individual’s education and previous employment, and perform internal and external reference checks. Where local labour law or statutory regulations permit, NewBanking may also conduct criminal and/or credit checks. The extent of background checks is dependent on the position.

Confidentiality Agreement & Acceptable Use Policy

Upon acceptance of employment at NewBanking, all employees are required to sign a confidentiality agreement and must acknowledge receipt of and compliance with our Acceptable Use Policy. The Acceptable Use Policy outlines our expectation that every employee will conduct business lawfully, ethically, and with respect for customers, partners, and fellow co-workers.

The confidentiality and privacy of customer information and data is emphasized in the introduction for new employees.

Awareness & Training

Employees are provided with security and privacy training as part of the introduction as well as during the course of the employment. Regular training is provided to ensure employees stay up to date on relevant security topics, threats and risks.

Depending on an employee’s job role, additional security training and policies may apply. NewBanking employees handling customer data are required to complete necessary requirements in accordance with these policies. Training concerning customer data outlines the appropriate use of data in conjunction with business processes as well as the consequences of violations.

Every employee is responsible for communicating security and privacy issues, concerns and suspected breaches to the CISO.

Security and Privacy Talk

On a regular basis, NewBanking engages internal and external speakers to address relevant security and privacy topics and threats in workshops to ensure that key employees are provided insight into current and future security challenges and opportunities that need to be addressed in the platform we provide.

Our Security and Privacy Team

NewBanking is, despite its small size, focusing on protecting the data we are entrusted by users and customers and therefore a Chief Information Security Officer (CISO) and Data Protection Officer (DPO) is appointed to drive the security improvement in the platform we provide and the way we work. The CISO and DPO are the main contacts for any security or compliance related questions, requests or concerns.

Third-Party Audits and Certifications

NewBanking has held an ISO27001 certification since March, 2021. Customers can receive a copy of the ISO27001 certificate upon request.

Operational Security

Vulnerability Management

NewBanking scans its IT environment with commercial tools on a regular basis to detect and in a timely manner take adequate actions to reduce and mitigate the risk they might expose the platform to. As soon as a vulnerability has been detected, it will be documented, prioritized based on severity and criticality, and assigned an owner with responsibility to determine appropriate actions to mitigate the risk. Decided actions will be documented, tracked and status will be followed up on a frequent basis until the risk has been reduced and mitigated to an acceptable level.

Malware Protection

A successful malware attack could lead to data being disclosed, unauthorised access being gained and accounts being compromised with a personal data breach as potential result. Therefore, all data uploaded to the platform is scanned for malware by industry leading malware protection solutions.

Monitoring and Alerts

NewBanking monitors the performance of the platform i.e. through a third party verifying the health of the platform to understand the level of availability and various security related activities i.e. alerts when a user logs in to production environment.

Security Incident Management

We have a rigorous security incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly affect user or customer data are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff and external partners are trained in forensics and handling evidence in preparation for an event, including the use of proprietary tools.

Data Center and IT Operations

NewBanking's platform is hosted in a state of the art data center and follows best practice IT operations processes and procedures. NewBanking utilizes the service of Digital Ocean for hosting and operations of the platform provided. Digital Ocean provides data center, hardware and services which are a fundamental part of the platform provided by NewBanking. The services provided by Digital Ocean are certified according to ISO27001 and their certificate can be reviewed on https://www.digitalocean.com/trust/certification-reports/

Disaster Recovery and Service Availability

To minimize service interruption due to hardware failure, natural disaster, or other catastrophes, NewBanking implements a disaster recovery program at all of its data centers (operated by Digital Ocean). This program includes multiple components to minimize the risk of any single point of failure, including the following:

- Data replication and backup: To help ensure availability in the event of a disaster, data is replicated to multiple systems within a data center (Amsterdam, The Netherlands), and also replicated to a secondary data center (Frankfurt, Germany).
- Digital Ocean operates a geographically distributed set of data centers that is designed to maintain service continuity in the event of a major incident or disaster.
- NewBanking has an IT Disaster Recovery Plan that will enable the organisation to recover the service/platform and data to normal operations within 72 hours.

- We conduct annual testing of our IT Disaster Recovery Plan.

Encryption at Rest and in Transit

To protect our platform against unauthorised disclosure of data, NewBanking has applied a concept of encryption at rest as well as in transit. This means that when data is sent to and from the platform, the data is encrypted using best practice HTTPS/TLS encryption algorithms. The data stored in the platform is strongly encrypted (AES256) at rest and done in addition to the database-level encryption performed by Digital Ocean to eliminate the risk of Digital Ocean's IT administrators, responsible for server maintenance, having access to the data.

NewBanking's encryption keys are managed in accordance with best practice key management which requires involvement from senior management at NewBanking to retrieve or regenerate the encryption keys.

Software Development

It is NewBanking's policy to consider the security properties and implications of the application, systems and services provided throughout the entire life cycle of the platform. NewBanking's Software Development Life Cycle (SDLC) calls for the development team to implement appropriate security measures in applications, systems, and services.

NewBanking employs a variety of measures to ensure that the applications, systems and services provided meet high standards of software security. This section outlines NewBanking's current approach to software security; it may adapt and evolve in the future.

Security is at the core of our design and development process, and we apply the concepts of security-by-design and security-in-depth. Our development team follows an agile software development methodology and addresses security in all stages of the SDLC from Requirements Gathering, Design, Build, Test, Deploy, Decommissioning, and Post Implementation Review.

The following activities ensure that security is addressed throughout the development: risk assessments, peer-review of design, adherence to secure coding guidelines (OWASP), peer code review, vulnerability scanning, penetration test, and QA review.

NewBanking has established a development, test and pre-production environment that is separated from the production environment. Production data is not used in any of the development, test or pre-prod environments; however, it might occasionally be used for problem and issue resolution.

Data Usage and Ownership

NewBanking users own their data, not NewBanking. The data that users put into our systems is theirs, and we do not sell it to third parties. We offer users the possibility to share personal data with our customers through consent on their own terms in a user friendly and efficient way. In the terms and conditions of our User Agreement, we outline details on data processing and describe our commitment to protecting user and customer data. It states that NewBanking will not process data for any purpose other than to fulfill our contractual obligations. Furthermore, if users delete their data, we commit to deleting it from our systems within 1 day if no other legal, contractual obligations exist between the user and our customer.

NewBanking might use the data (anonymised and aggregate) for statistical purposes to gain insight into usage of features and to drive improvement of the platform, user experience (e.g. send notification to update data when data, e.g. a password or driver's license, has expired or otherwise reached its end of retention) and quality of the data.

Finally, we provide tools that make it easy for customers to take their data with them if they choose to stop using our platform, without penalty or additional cost imposed by NewBanking.

Access to Data

Individual Access to Data

Individuals signing up to the NewBanking platform are able to share their data with customers of the platform (normally through a consent) or any other third party not on the platform. Individuals have access to their own data and are able to add and remove the data as long as it is in line with provided consents or other contractual, legal and regulatory obligations the individual entered into with customers or authorities.

NewBanking Access to Data

Only a small group of NewBanking employees (currently only the CTO) have access to customer data. For NewBanking employees, access rights and levels are based on their job function and role, using the concepts of need-to-know and least-privilege to restrict access privileges to assigned responsibilities.

NewBanking employees are only granted a limited set of default permissions to access company resources. Requests for additional access follow a formal process that involves a request and an approval from senior manager as dictated by NewBankings access control policies. Approvals are managed electronically and records are maintained for traceability and audit purposes.

NewBanking employee access is adjusted when job responsibilities change or when employment is terminated; in addition, all employee access is reviewed on a regular basis.

Customer Access to Data

Each customer organization appoints one or more administrators (who are encouraged to use multi-factor-authentication when logging on to the platform) to manage customer specific settings and to administer user roles and privileges within their own organization. General users within the customer organization are expected to be provided access based on the principles of need-to-know and least privilege.

Third-Party Supplier Access to Data

NewBanking engages third-party suppliers to verify and enrich the data provided by the individual or customer. Third-party suppliers are only provided access to data that is relevant for the specific task they have been assigned which could be to verify the identity of the individual using the platform by passport or driving license validation.

Third-Party Supplier Management

NewBanking is responsible for all data processing activities related to our platform. However, NewBanking may engage third-party suppliers to provide services related to NewBanking platform, including data center operation, customer and technical support, security testing and audits etc.

Prior to onboarding third-party suppliers, NewBanking conducts an assessment of the security and privacy practices of the suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide.

Once NewBanking has assessed the risks related to the third-party supplier, the supplier is required to enter into contractual terms covering appropriate security, confidentiality and privacy requirements.

Requests from Law Enforcement

The user, as owner of the information, is primarily responsible for responding to law enforcement data requests; however, like other technology and communications companies, NewBanking may receive direct requests from governments and courts around the world about how a person has used the company's platform. We take measures to protect user privacy and limit excessive requests while also meeting our legal obligations. Respect for the privacy and security of data that people and companies store with NewBanking remains our priority as we

comply with these legal requests. When we receive such a request, our team reviews the request to make sure it satisfies legal requirements and NewBanking's policies.

For NewBanking to comply, the request must be made in writing, signed by an authorized official of the requesting authorities and issued under an appropriate law.