UNDERBILAGA B: SÄKERHET

1 INTRODUCTION

1.1 The goal of this document is to provide transparent, high-level information to Kivra's stakeholders about Kivra's commitment to information security. The document describes Kivra's information security responsibilities and undertakings regarding both the services that Kivra provides to Senders (Sw. *Avsändare*), i.e. the Delivery Service (Sw. *Förmedlingstjänsten*) and any Additional Services (Sw. *Tilläggstjänster*) as well as the services that Kivra provides to Users (Sw. *Användare*). i.e. the digital mailbox (Sw. *digitala brevlådan*). These services are in this document together referred to as the "**Kivra Platform**".

1.2 As Kivra may change its security measures over time, this document may be revised accordingly. Partners and Senders of Kivra can always receive the latest version of this document by contacting Kivra's Security Team as security@kivra.com.

2 KIVRA'S CORPORATE TRUST COMMITMENT

Kivra is committed to achieving and maintaining the trust of our stakeholders. Our goal is to be as transparent as possible with our stakeholders in offering security to meet and exceed expectations in today's ever changing tech landscape.

3 GOVERNANCE

3.1 Policy Ownership

Kivra has a documented Information Security Policy that all employees must read and acknowledge. This policy is approved by the Board of Directors, reviewed and updated annually. Information Security Policy development, maintenance, and issuance is the responsibility of the Kivra CISO.

3.2 Kivra Infrastructure

Kivra hosts the Kivra Platform in a hybrid-cloud environment. Content is hosted in multiple on-premise data centers located within Sweden. The data center facilities are provided by Swedish suppliers, all hardware and software is owned by Kivra and maintained by either our employees or consultants contracted directly by Kivra.

3.3 Third-Party Architecture

Kivra may use one or more third-party suppliers. When doing so, Kivra contractually ensures that these third parties follow adequate security requirements.

Kivra has Risk Management procedures in place that take integrations with, and solutions from, third parties into account on a service/system level. This is governed by the Information Security Policy and the Third Party Risk Management Instruction.

3.4 Audits, Certifications, and Regulatory Compliance

Kivra is connected to the infrastructure Mina meddelanden, governed by the Agency for Digital Governance ("**DIGG**"). As such, Kivra is regularly audited by DIGG towards their ISO27001-based information security requirements.

Kivra's information security is governed by an Information Security Management System (ISMS) that adheres to the ISO 27001 standard.

4 SECURITY CONTROLS

4.1 Organization of Security

Kivra's COO is responsible for the overall Information Security Management of the Kivra Platform, including oversight and accountability. This responsibility is enforced by the Kivra CISO who answers directly to the Kivra COO and leads a Security Team that consists of a Security Subject Matter Expert, Security Engineers and Infrastructure Security. All Business Function/System Owners (Product Owners and Engineering Managers) have Information and IT Security responsibilities within their roles.

The Physical and Personal security of Kivra's offices and employees is the responsibility of the Kivra COO, also coordinated by the Security Team.

4.2 Asset Classification and Logical Access Control

- Kivra maintains an inventory of essential information assets such as servers, databases, and software governed by the IT Policy and the IT Asset Management Instruction.
- Kivra adopts the principle of least privilege for all accounts running application or database services, as well as with its own staff.
- Kivra maintains separate development, sandbox (UAT), staging and production environments. Access to each environment and within each environment is separated and strictly controlled.
- All access to Kivra's servers or data is logged and can only be accessed using multifactor authentication or by users using Mobile Bank-ID.
- Kivra's HR onboarding and off-boarding processes handle provisioning and de-provisioning of accounts and access.
- Audits on accounts and access are performed regularly.

4.3 Personnel Security and Training

- All employees at Kivra sign a confidentiality agreement when their employment begins. In addition, Kivra conducts background checks for system administrators, developers and other users with privileged access as part of its onboarding process. This also includes key roles within the Kivra Management Team.
- All employees are informed of, and agree to comply with, Kivra's IT- and Information Security policies and practices as a part of their initial on-boarding.
- All Kivra employees undergo security and privacy training as part of their on-boarding and receive frequent training sessions focusing on specific subjects such as phishing.
- Kivra conducts frequent awareness related tests and communicates security related information to all employees and consultants through several internal communication channels.

4.4 Physical and Environmental Security

- Access to Kivra facilities is controlled by 24-hour security. Additionally, all Kivra offices are protected by locked access and are under 24-hour video surveillance (recording triggered by motion). All Kivra employee workstations are encrypted and password protected, and all Kivra user accounts require two-factor authentication.
- Data centers facilities and physical security are provided by Swedish suppliers complying with Kivra contractual requirements.

4.5 Policies and Logging

The Kivra Platform is operated in accordance with the following procedures to enhance security:

- All processing of content is logged monitoring user activity and potential anomalies.
- API key information for third-party services provided by the Sender are encrypted for storage.
- Kivra keeps audit logs for all access to production servers.
- Server access is controlled via public key access, instead of passwords.
- Logs are stored in a secure centralized host to prevent tampering.
- Kivra application and ssh audit logs are stored for five years.
- Passwords are not logged under any circumstances.
- Access to Kivra mail and document services is only allowed on approved workstations and mobile devices that have automated security policies enforced.

4.6 Intrusion Detection

Kivra monitors system, user, and file behavior across its infrastructure using a host-based Intrusion Detection System. Intrusion Detection alerts are monitored by the Security Team and an external SOC.

Kivra's APIs use strict role-based access controls and user permissioning. Unauthorized web requests and API calls are logged and alerts are handled by Kivra's engineering team.

4.7 Security Logs

All Kivra systems used in the provisioning of the Kivra Platform, including firewalls, routers, network switches, and operating systems log information to their respective system log facility or a centralized log server (for network systems) in order to enable security reviews and analysis. Kivra has automated alerts and searches on these logs.

4.8 System Patching and Configuration Management

Kivra patches its servers on a regular basis, which ensures that the latest patches for the software we use are applied. Kivra's configuration management system regularly applies configuration based on repositories.

Kivra maintains multiple environments and tests changes in containerized development environments and in live staging environments before making changes to production environments.

4.9 Vulnerability Management

Kivra's infrastructure and applications are continuously scanned for vulnerabilities. Alerts are monitored by our Security Team. Kivra also maintains a list membership to various CVE vulnerability mailing lists. Patches and vulnerabilities are remediated based on severity. This is governed by the Information Security Policy and the Vulnerability Management Instruction.

In addition, Kivra integrates security into its development process by utilizing static code analysis tools to identify potential vulnerabilities in our codebase before deployment.

4.10 Third-Party Penetration Testing

Kivra undergoes a third-party penetration test of the Kivra Platform on an annual basis. Kivra also conducts our own internal penetration tests in relation to significant changes in our services and environment.

4.11 Monitoring

For technical monitoring, maintenance and support processes, Kivra uses a combination of tools to ensure that processes and servers are running properly, including but not limited to:

- Process monitoring
- CPU, disk, and memory monitoring
- Uptime monitoring
- Functional monitoring
- Database monitoring
- Application Tracing
- Error monitoring
- Office monitoring

4.12 External Access Control

The Kivra Platform employs a variety of security controls. These include, but are not limited to:

- Receiving Users log in to the Kivra Platform using Mobile Bank-ID.
- Senders log in to the Kivra Platform using Google Authentication or OTP.
- All web services use encrypted HTTPS for all traffic and disallow all HTTP traffic via HTTP Strict Transport Security ("HSTS").
- Kivra does not use persistent cookies for sessions.
- Sessions expire after a few hours of inactivity.

- Failed login attempts are recorded and an account is locked out with the owner notified after multiple failed attempts.
- Kivra's REST APIs are accessed with separate API keys, which can only be provisioned by Kivra Sender user accounts with administrative access. API keys are granted access to specific API endpoints when created.

4.13 Development and Maintenance

Kivra uses third party tools to effectively manage the development lifecycle. During testing, Kivra generates sandbox accounts and fake data for testing. Kivra does not use production data in sandbox accounts.

Application source control is accomplished through private repositories. Kivra has controls in place to ensure that all code changes are reviewed and implemented by at least two developers before being merged to Kivra's main code branch.

Kivra maintains a list of core security principles for engineering and high-level guidelines on security topics for secure software development.

4.14 Malware Prevention

As a mitigating factor against malware, all Kivra servers run LTS editions of Operation Systems, as well as malware protection functionality.

Kivra provides proper change management to ensure that only authorized packages are installed via a package management system containing only trusted software, and that software is never installed manually.

All Kivra employee workstations are provided with virus scanners and updated definitions sent out from a central device management platform.

4.15 Information Security Incident Management

Kivra maintains written and regularly tested incident management instructions and procedures. Kivra has 24x7x365 on-call incident management staff. Kivra uses tools to ensure complete coverage with defined escalation policies.

4.16 Data Encryption

The Kivra Platform uses industry-accepted encryption practices to protect Sender data and communications during transmissions between a Sender's network and the Kivra Platform and at rest.

4.17 Return and Deletion of Kivra User Data

The Kivra Platform allows import, export, and deletion of Kivra User data by authorized users at all times during the term of a Kivra User's subscription. Following termination or expiration of the Kivra User subscription, Kivra shall securely overwrite or delete Kivra User data within 20 days following any such termination, in accordance with Kivra's General Terms and Conditions.

4.18 Reliability and Backup

All networking components, SSL accelerators, load balancers, web servers and application servers are configured in a redundant configuration. All Sender data submitted to the Kivra Platform is stored on a primary database server with multiple active clusters for higher availability. All database servers replicate in near real-time and are backed up on a regular basis. Backups are encrypted using AES-256 encryption and verified for integrity.

4.19 Business Continuity Management and Disaster Recovery

Kivra has documented Business Continuity procedures. Normal backups are stored in backup servers on-site.

Clusters containing User data use replication to other sites and duplication factors to ensure data redundancy. We also use life-cycle policies to ensure a “delete all scenario” is impossible.

4.20 Mobile Device Management Policies

Kivra uses Mobile Device Management (“**MDM**”) platforms to control and secure access to Kivra resources on mobile devices such as phones, tablets, and laptops. Kivra enforces common security settings such as, but not limited to, encryption, lock screen passwords, password expiration, display timeouts, and remote location and remote wipe.

4.21 Blocking Third Party Access

The Kivra Platform has not been designed to include any backdoors or similar functionality that would allow the government or any third parties to access data. We do not provide any government or other third party with encryption keys, or any other way to break our encryption.

5 CONTACTS

Kivra’s Security Team can be reached by emailing security@kivra.com.