GSMValve OÜ (Navirec)

Information Security Policy

Document title	Information Security Policy
Owner	GSMValve OÜ (Navirec) — IT Department
Approved by (Management)	Hans Alter
Reviewed by (IT Manager)	Margus Paurson
Version	1.0
Effective date	13.05.2026
Review cycle	Annual, or upon material change

1. Purpose

This Information Security Policy sets out the principles, responsibilities and minimum requirements that GSMValve OÜ (operating as Navirec) follows to protect the confidentiality, integrity and availability of the information it processes — including personal data processed on behalf of customers and partners. It is the top-level information security policy of the company and is supported by underlying procedures, technical standards and records.

This policy is aligned with the relevant principles of ISO/IEC 27001:2022 and ISO/IEC 27002:2022, and is intended to demonstrate compliance with applicable data-protection legislation, including the EU General Data Protection Regulation (GDPR).

2. Scope

This policy applies to:

- All employees, contractors, interns and third parties acting on behalf of GSMValve OÜ.
- All information assets owned, processed, stored or transmitted by GSMValve OÜ, in any format (digital, paper, verbal).
- All IT systems, applications, networks, cloud services and physical facilities used to deliver the Navirec service.
- All sub-processors and suppliers with access to GSMValve OÜ data or systems.

3. Roles and Responsibilities

- **Management** is accountable for information security, approves this policy, and ensures sufficient resources are available.
- **IT Manager (Margus Paurson)** is the designated security officer. Responsible for implementing, maintaining and monitoring this policy and the supporting controls.
- **All staff and contractors** are responsible for complying with this policy, completing required security awareness training, protecting credentials, and reporting suspected security incidents without delay.
- **Developers** are responsible for following the secure-development requirements set out in section 9.

4. Information Classification and Handling

Information processed by GSMValve OÜ is classified as Public, Internal, Confidential or Personal Data. Personal Data and Confidential information must only be accessed by authorised personnel on a need-to-know basis, must be stored within approved systems, and must not be transferred outside the EU/EEA unless appropriate safeguards (such as Standard Contractual Clauses or an adequacy decision) are in place.

Customer data is logically segregated at the application layer. Each customer operates as a separate tenant, and access to a customer's data is determined by the rights granted to that customer's own users; commingling of data between customers is prevented by application-level access controls.

Before any non-public information is disclosed to an external party, the identity and authorisation of the recipient is verified through an established channel — for example, the customer's nominated contact, a signed instruction, or a previously authenticated communication channel. Casual or unverified channels are not used for the disclosure of confidential or personal data.

5. Access Control and Authentication

- Each user has a unique personal account. Shared accounts are prohibited.
- Access to systems and data is granted on a least-privilege, need-to-know basis and is reviewed at least annually.
- Passwords must meet a documented complexity standard (minimum length, character variety, blocking of common passwords) and are enforced by the platform.
- Remote access to internal systems is permitted only through the corporate VPN, using personal credentials.
- Joiner, mover and leaver changes (account creation, role change, revocation) are performed promptly and recorded.
- Where external parties (e.g. IT support, contractors, vendors) require access to GSMValve OÜ systems, access is granted on a named-account basis, is time-limited, is recorded, and is contingent on a written confidentiality agreement being in place. External access is reviewed regularly and revoked when no longer required.

6. Cryptography

- **Data in transit:** all access to Navirec services and APIs is encrypted using TLS 1.2 or higher. Administrative access uses an encrypted VPN.
- **Data at rest:** personal data stored on company systems is protected by appropriate technical safeguards. Company-issued endpoints use full-disk encryption.
- **Key management:** cryptographic keys and secrets are stored in protected key stores and are not embedded in source code.

7. Physical and Environmental Security

Production servers are operated by Elisa Eesti AS, the primary hosting and managed-infrastructure provider, and are physically located in Greenergy Data Centers (Tallinn) — a facility with 24/7 monitored access, biometric and ID-based entry controls, environmental controls and uninterruptible power supply (UPS). Physical access to racks is restricted to authorised personnel. Office workstations are protected by screen-locking, clean-desk practice and locked storage for paper records where applicable.

8. Operations Security

- **Patch and vulnerability management:** operating systems, dependencies and container images are kept up to date. Known vulnerabilities are tracked and remediated according to risk.
- **Malware protection:** all company-issued endpoints run an approved endpoint security solution (currently ESET Small Business Security).
- **Logging and monitoring:** security-relevant events from production systems are logged centrally, protected against tampering, and retained for forensic analysis in line with the documented retention standard (target: at least 180 days for security logs).
- **Backups:** production data is backed up, replicated and restore-tested on a recurring basis.
- **Secure disposal:** storage media containing personal or confidential data is securely erased or destroyed before reuse or disposal.

9. Secure Software Development

- Development, testing and production environments are logically separated.
- Developers do not have direct write access to the production environment; all changes go through a controlled change-management process with review, testing and rollback capability.
- The development process addresses, at a minimum, the current OWASP Top 10 risks (e.g. injection, broken access control, security misconfiguration).

- Dependencies are reviewed for known vulnerabilities; updates are applied as part of the regular release cycle.

10. Supplier and Sub-processor Security

Suppliers and sub-processors that process personal data on behalf of GSMValve OÜ are subject to a written data-processing agreement and, where applicable, EU Standard Contractual Clauses. A current sub-processor list is maintained and provided to customers on request.

11. Incident Management

All staff and contractors are required to report any suspected or confirmed security incident to the IT Manager without delay. Incidents are recorded, contained, investigated and remediated, and lessons learned are fed back into this policy and supporting procedures. Personal-data breaches that are likely to result in a risk to data subjects are reported to the relevant Data Protection Authority within 72 hours, and affected customers (data controllers) are notified in accordance with contractual obligations.

12. Business Continuity and Disaster Recovery

GSMValve OÜ maintains business-continuity and disaster-recovery arrangements proportionate to the risks of its operations, including data replication, UPS-protected hosting, and periodic restore testing. Continuity arrangements are reviewed and tested on a recurring basis and updated when material changes occur.

13. Personnel Security, Awareness and Training

Before granting access to systems or personal data, candidates undergo identity verification and, where appropriate to the role, reference and background checks. Employment and contractor agreements include written confidentiality and information-security obligations that take effect on the first day of access and remain in force after termination.

All personnel with access to personal data receive security-awareness training at onboarding and at least annually thereafter. Training covers acceptable use, password and credential hygiene, phishing, data-handling rules, secure remote working, and how to recognise and report security incidents.

14. Confidentiality

All employees and contractors are bound by written confidentiality obligations covering customer and personal data. These obligations remain in force after termination of the employment or contractual relationship.

15. Compliance, Audit and Review

Compliance with this policy is monitored by the IT Manager. Tamper-evident audit trails are maintained for security-relevant actions affecting customer data and are protected against unauthorised modification or deletion.

In addition to the annual policy review, periodic random spot-checks are performed by the IT Manager on access logs, account permissions, change-management records and backup-restore evidence, to confirm that security controls are operating as intended. Findings from these checks are recorded and any required corrective actions are tracked to completion.

The policy and the controls supporting it are reviewed at least annually, after any material incident, and when significant changes occur in the technology, organisation or applicable regulation. Non-compliance with this policy may result in disciplinary action, up to and including termination, and in the case of contractors, termination of the engagement.

16. Approval

This Information Security Policy is approved by the management of GSMValve OÜ and is effective from the date stated below.

Role	Name	Signature / Date
Approved by (Management)	Hans Alter	*digitally signed*
Reviewed by (IT Manager)	Margus Paurson	*digitally signed*