SMSBAT

TECHNICAL & ORGANIZATIONAL MEASURES (TOMs)

SMSBAT
NEW POSSIBILITIES

TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs)

Framework: Based on ISO/IEC 27001 and NIST Standards

Security

1. Information Security Organization

- **ISMS Framework:** Information security is managed through a comprehensive Information Security Management System (ISMS).
- **Leadership & Governance:** Strategic objectives are set by the Management Board, while operational execution is led by the Chief Information Security Officer (CISO) and the Chief Privacy Officer (CPO).
- **Risk Management:** Internal and external threats are identified and prioritized using a formal methodology aligned with ISO 31000 and the COSO framework.
- **Policy Compliance:** Security policies and procedures are formally approved, communicated to all employees, and subject to periodic reviews.

2. Data Protection & Cryptography

- **Encryption In-Transit:** All data transmitted via public networks is protected using modern cryptographic protocols, including HTTPS, IPSec VPN, SMPP over SSL/TLS, and SFTP.
  +4
- **Encryption At-Rest:** Sensitive information, message content, and backup archives are encrypted using the **AES-256** standard.
  +1
- **Standard Alignment:** Cryptographic mechanisms follow leading international practices, specifically NIST Special Publication 800-175B.

3. Access Control & Identity Management

- **Least Privilege Principle:** Access to systems and data is granted based on the "need-to-know" principle and the minimal set of required privileges.
- **Multi-Factor Authentication (MFA):** Remote access requires a secure VPN connection with 2FA and additional authentication for cloud applications.
  +1
- **Identity Tracking:** Every interaction with ICT systems is traced to a unique, personalized user identification to ensure accountability.

4. Operations & Network Security

- **Environment Segregation:** Development, testing, and production environments are strictly segregated to prevent unauthorized changes to the operational environment.
- **Network Segmentation:** Networks are divided into segments (e.g., DMZ, internal, restricted) filtered by security devices to permit only approved traffic.
- **Vulnerability Management:** Continuous monitoring for technical vulnerabilities is performed through automated scanners, penetration testing by independent specialists, and bug bounty programs.
  +2

5. Physical Security & Data Sanitization

- **Secure Infrastructure:** Data processing facilities are protected by security perimeters, surveillance, and physical access controls (gates, locks, barriers).
  +1
- **Media Sanitization:** When disposing of assets or deleting data, Infobip follows **NIST Special Publication 800-88** guidelines to prevent unauthorized data retrieval.
- **Deletion Certification:** Upon customer request, a written certificate can be issued to confirm the completion of data deletion.

6. Incident Management & Continuity

- **Rapid Response:** Dedicated incident response teams monitor systems 24/7 to identify and mitigate security events.
- **Customer Notification:** Customers are notified of confirmed security incidents affecting their data as soon as possible, no later than 72 hours after classification.
- **Business Continuity:** Redundancy and high-availability techniques are implemented to ensure service availability even during adverse situations.

7. Certifications & Compliance

The platform's security maturity is verified by the following international certifications:

- **ISO/IEC 27001** (Information Security Management System).
- **ISO/IEC 27017 & 27018** (Cloud Security & PII Protection).
- **AICPA SOC2 Type I**.
- **CSA STAR Level 1** & **NCSC Cyber Essentials**.

Contacts

To order a presentation or get a consultation, contact us:
help@smsbat.com, www.smsbat.com