SalesScreen Security & Compliance Overview

Version: 1.0
Last Updated: 2025-05-28

Introduction

At SalesScreen, we prioritize security and privacy to ensure the protection of our customers' Customer Data. This document outlines our approach to security, detailing the technical and organizational measures we have in place to safeguard information, comply with industry regulations, and maintain customer trust.

Security Governance & Compliance

Security at SalesScreen is built on a strong governance framework that aligns with recognized industry standards, including ISO 27001 and GDPR. We have established comprehensive policies, procedures, and controls to manage security risks effectively. Regular audits and continuous improvements ensure that we remain ahead of emerging threats and regulatory changes.

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

As an ISO 27001-certified organization, we maintain a structured Information Security Management System (ISMS) that includes documented policies, rigorous risk assessments, and ongoing compliance monitoring. By regularly reviewing and updating our security controls, we ensure that our approach evolves in line with industry best practices.

SECURITY POLICIES

To maintain a secure operating environment, we have implemented a range of policies that govern how we protect data and respond to security incidents, including:

- Our Information Security Policy defines the core principles that guide our security practices.

- A structured Incident Management Procedure ensures that any security event is promptly detected, assessed, and resolved.
- We enforce an Access Control Policy based on the principle of least privilege, ensuring that users only have access to the data and systems necessary for their roles.
- Our Secure Software Development Policy embeds security best practices into every stage of our software development lifecycle.
- The Business Continuity & Disaster Recovery Plan safeguards against disruptions, helping us maintain operational resilience.

Technical Security Measures

Protecting Customer Data requires a multi-layered security approach, covering encryption, system resilience, access controls, and threat detection.

DATA ENCRYPTION & PSEUDONYMIZATION

We apply encryption and data protection mechanisms to safeguard sensitive information:

- All data transmitted to and from SalesScreen is encrypted in transit using TLS 1.2+.
- Customer Data is encrypted at rest using AES-256 encryption.
- Data anonymization and pseudonymization techniques are employed where applicable to enhance privacy.

SYSTEM AVAILABILITY & RESILIENCE

To ensure high availability, our platform is hosted on Microsoft Azure, leveraging redundant infrastructure and geographic failover between EU data centers. Our Disaster Recovery Plan includes automated failover mechanisms and proactive resource scaling, allowing us to maintain reliable service even during unexpected incidents. Security patching and system-hardening practices are regularly applied to mitigate vulnerabilities. For our Enterprise customers, we provide a SLA guaranteeing 99.5% uptime.

BACKUP & DATA RECOVERY

Regular automated backups are performed to ensure data availability and integrity. Our backup strategy includes both incremental and full backups, stored securely in multiple geographic locations. Backup data is encrypted, and periodic restore tests are conducted to validate the effectiveness of our recovery procedures.

ACCESS CONTROL & AUTHENTICATION

Access to our systems follows a Zero Trust security model, requiring authentication and authorization for every request. We enforce Multi-Factor Authentication (MFA) across all critical systems and provide Single Sign-On (SSO) for a seamless yet secure login experience. Role-Based Access Control (RBAC) ensures that users only have the permissions necessary for their responsibilities, while regular access reviews help revoke any outdated privileges.

SECURITY MONITORING & THREAT DETECTION

We continuously monitor our production environments to detect and respond to security threats. Our proactive security measures include regular vulnerability scanning, penetration testing, and real-time audit logging to track access and system changes. To further strengthen our defenses, we deploy endpoint protection solutions that incorporate anti-malware and intrusion detection systems.

NETWORK SECURITY

SalesScreen employs multiple layers of network security controls to protect against unauthorized access and attacks:

- A Web Application Firewall (WAF) safeguards our services from web-based threats, including SQL injection and cross-site scripting (XSS).
- Built-in Distributed Denial of Service (DDoS) protection ensures service availability by mitigating large-scale attacks.
- Network segmentation limits access between environments to reduce the risk of lateral movement.

PENETRATION TESTS

We engage third-party security experts to conduct application-level and infrastructure-level penetration tests at least annually.

DATA SEGREGATION

SalesScreen is a multi-tenant platform that implements both physical and logical controls to ensure the separation of Customer Data. For Enterprise customers requiring additional isolation, SalesScreen offers the option of a dedicated SQL database, which may incur additional costs.

Other customers are hosted across a collection of multi-tenant databases, where logical separation is enforced. Customer Data is consistently tagged with a unique customer identifier, which is used throughout the platform to segregate data ownership and control access. SalesScreen's application programming interfaces (APIs) are designed to recognize these identifiers and enforce strict authorization controls, ensuring that users and systems can only access data associated with their own organization.

Organizational Security Measures

Beyond technical safeguards, we invest in training, secure development practices, and a structured incident response strategy to create a culture of security awareness.

PHYSICAL SECURITY

SalesScreen enforces strict physical security controls to protect company assets and data:

- Our cloud infrastructure is hosted in Microsoft Azure data centers, which maintain industry-leading physical security measures, including biometric access controls, surveillance, and on-site security personnel.
- Employee devices are managed using endpoint security solutions to prevent unauthorized access.
- Remote work security policies ensure that devices connecting to SalesScreen systems comply with security standards, including full-disk encryption and enforced screen-locking.

- Office security measures include badge-restricted access, visitor logging, and secure disposal of sensitive documents.

EMPLOYEE SECURITY AWARENESS & TRAINING

All employees undergo mandatory annual security and privacy training, supplemented by phishing awareness campaigns and simulated social engineering attacks. Our security policies also provide clear guidelines on acceptable use, data handling, and incident response to ensure company-wide adherence to best practices.

BACKGROUND CHECKS

All SalesScreen employees undergo background checks prior to employment, and periodically as appropriate for their role, in accordance with local laws and regulations. These checks may include criminal record verification, employment history, and reference checks, particularly for roles with access to sensitive Customer Data or systems.

SECURE SOFTWARE DEVELOPMENT LIFECYCLE (SDLC)

Security is an integral part of our software development process. We incorporate code reviews and automated security testing into our CI/CD pipelines, allowing us to detect and remediate vulnerabilities early. Our development team follows secure coding guidelines based on OWASP principles and other industry best practices.

INCIDENT RESPONSE & RECOVERY

We maintain a well-defined incident response plan with 24/7 monitoring capabilities to ensure rapid detection and resolution of security incidents. In the event of a breach, our structured escalation procedures enable swift containment and mitigation. Post-incident reviews help us learn from past events and refine our security strategy to prevent recurrence. We have a public status page where customers can subscribe to updates concerning incidents that affect the availability of the platform.

Data Protection & Privacy

We are committed to protecting Customer Data through strict data minimization, retention, and privacy controls that align with global data protection regulations, including the GDPR.

DATA MINIMIZATION & RETENTION

Our data collection practices are designed to limit the information we process to what is strictly necessary. When a customer terminates their account, we delete or return their Customer Data within 30 days upon request. In the absence of such a request, Customer Data is securely deleted from production systems within 90 days following contract termination (unless a different retention period is mutually agreed upon in the customer agreement), in line with our data retention schedule and to ensure compliance with data retention policies.

DATA SUBJECT RIGHTS & PRIVACY CONTROLS

Customers have full control over their Customer Data, with the ability to access, correct, and delete personal information as needed. Our platform ensures logical data segregation to prevent cross-customer access, and we fully comply with GDPR requirements for data portability and erasure.

Third-Party & Vendor Security

To maintain the security of our extended ecosystem, we carefully assess and monitor the security posture of our third-party service providers.

VENDOR RISK MANAGEMENT

Before on-boarding any third-party provider, we conduct thorough risk assessments to evaluate their security capabilities. Sub-processors are contractually required to adhere to strict security controls, and we regularly review their compliance through audits and security evaluations.

SUB-PROCESSOR ACCOUNTABILITY

We ensure that any sub-processors handling Customer Data do so only within the scope of agreed-upon services. Access is strictly limited to what is necessary, and SalesScreen remains fully accountable for ensuring that sub-processors comply with our security and data protection obligations. A list of our current sub-processors is maintained and can be provided to customers upon request or as part of our Data Processing Addendum (DPA).

Conclusion

At SalesScreen, security and compliance are fundamental to our operations. Through a combination of robust technical controls, strong governance practices, and a proactive security culture, we protect the confidentiality, integrity, and availability of Customer Data. We continuously evaluate and enhance our security measures to stay ahead of evolving threats and regulatory requirements.

For further inquiries, please contact our Security Team at security@salesscreen.com.