liana

# Information Security Guidelines

# Table of contents

**Introduction** **3**

Company Overview 3

Purpose of the Document: 3

Developer documentation 4

**Regulatory Compliance and Security Governance** **5**

Regulatory compliance 5

Security Governance Structure 5

Standards and certifications 6

**Access control** **7**

Minimum Rights Policy and Role-Based Access 7

Ownership and Management of Systems 7

**Data protection** **8**

Data Segregation 8

Encryption in Transit and Backup 8

Data Loss Prevention Measures 8

**Security Monitoring and Auditing** **10**

System Availability Monitoring and Logging 10

Isolated Management of Logs, Metrics, and Alarms 10

Security Audits and Assessments 11

**Business Continuity and Disaster Recovery** **12**

Continuous Support and Availability 12

Automated Software Deployment for Business Continuity 12

Ensuring Resilience and Recovery 13

**Closing Statement** **14**

# Introduction

## Company Overview

Liana Technologies is a European software company founded in 2005. We specialize in digital marketing and communication software. Liana's marketing technology stack is used by more than 3,500 customers worldwide including companies such as Hertz, Toyota, Ikea and Starbucks. Our mission is to help our customers to accomplish their goals and get results with our marketing and PR technology. Our ambition is to grow to be the biggest marketing technology provider in the Nordics.

## Purpose of the Document:

The purpose of the information security guidelines document is to provide our customers with comprehensive insights into how Liana Technologies approaches and implements security measures across our suite of digital marketing and communication products. This document aims to reassure our customers about the customer robustness of our security infrastructure and practices. It serves as a resource to elucidate our commitment to maintaining the confidentiality, integrity, and availability of the customers' data while utilizing our services.

Through this document, we aim to:

- Transparently Communicate Security Practices: Detail our approach to information security, encompassing policies, procedures, and frameworks implemented to safeguard sensitive data.
- Assure Compliance and Standards: Highlight our adherence to industry standards, regulatory requirements, and certifications to foster trust and confidence in our customers.
- Empower Customer's Decision-Making: Provide valuable information for customers evaluating our services, enabling them to assess the security measures in place and make informed decisions regarding their partnership with Liana Technologies.

- Facilitate Collaboration: Establish a foundation of trust and cooperation by sharing our security principles, thereby fostering a collaborative approach to maintaining a secure environment for our customers.

This document serves as a testament to our commitment to information security and acts as a reference guide for our customers seeking assurance regarding the protective measures embedded within our services. To protect our customers, we do not publish low-level security configurations.

Liana reserves the right to update this Information Security Policy and may make changes to it as necessary.

# Developer documentation

At Liana, our employees are at the core of information security. However, as we focus on delivering SaaS software, we need to pay extra attention to application security. The field of software development is really fast paced. To ensure that our development teams focus on the right aspects, we maintain an internal handbook, The Liana DevOps handbook, which is the up-to-date version of the how-to in development, especially focusing on security aspects.This handbook consists of information e.g.:

- Currently approved security practices / DOs and DON'Ts of application development
- Technical baseline to ensure security and business continuity of our products
- End Of Life (EOL) actions to be monitored

# Regulatory Compliance and Security Governance

## Regulatory compliance

At Liana Technologies, we prioritize adherence to all applicable laws and regulations governing data security, privacy, and information management. Our commitment extends to ensuring compliance with regional, national, and international standards, safeguarding our customer’s data and upholding their trust.

Our approach to regulatory compliance encompasses:

- Data Protection Regulations: Ensuring alignment with data protection laws such as GDPR, CCPA, and other regional mandates.
- Privacy Standards: Implementing measures that align with global privacy standards to ensure data protection
- We continuously monitor evolving regulatory landscapes to adapt our policies and practices, ensuring ongoing compliance with emerging requirements.

## Security Governance Structure

At Liana Technologies, our security governance is built upon a robust triad comprising our CEO, CTO, and Data Protection Officer (DPO). This triad forms the cornerstone of our security decision-making process, ensuring a holistic and strategic approach to information security management.

Key aspects of our security governance include:

- Executive Leadership Involvement: Active participation of our CEO and CTO in shaping and overseeing security strategies.
- Data Protection Officer (DPO): The DPO is responsible for overseeing compliance, guiding privacy initiatives, and ensuring alignment with regulatory mandates.
- Security Awareness and Training: We emphasize maintaining a high level of employee security awareness through regular training, workshops, and educational programs. This ensures that all staff members are equipped with the knowledge and skills necessary to contribute to our security posture.

Our governance structure is designed to foster a culture of security consciousness across all levels of the organization, promoting proactive measures to mitigate risks and uphold the integrity of our customer's data.

Yet, the cornerstone of our security posture is a culture of security minded individuals, both in development and across the organization.

# Standards and certifications

Liana Technologies is committed to providing a secure environment for its customers' information. While we do not hold any official industry certifications, we adhere to the principles and practices outlined in leading certifications, such as ISO/IEC 27001, to ensure the protection of our environments.

# Access control

## Minimum Rights Policy and Role-Based Access

At Liana Technologies, access to all systems and data follows a strict Minimum Rights Policy. This policy ensures that individuals within the organization have access only to the information necessary for their roles and responsibilities.

Role-Based Access. Access is typically granted based on predefined roles. Employees are granted access rights according to their job roles, reducing unnecessary access privileges.

Our commitment to stringent access control mechanisms ensures the confidentiality and integrity of our customers' data, mitigating the risk of unauthorized access or data breaches.

## Ownership and Management of Systems

Every system within Liana Technologies, regardless of it being an internally developed system or a third-party service, is owned and managed by designated personnel within the organization. This approach ensures accountability and oversight for the security and functionality of each system.

Production Systems and Data Access. Access to production systems, especially where customer data resides, is strictly limited to authorized personnel mandated to handle and maintain these systems. Access rights are rigorously managed and regularly reviewed to ensure compliance with security protocols and regulatory compliance. The number of people having access to production data is kept as low as possible that still enables us to maintain and develop our systems.

# Data protection

## Data Segregation

At Liana Technologies, we uphold a strict segregation policy between our proprietary data (Liana's) and our customers' data, even within our multi-tenant systems. Our systems are architecturally designed to ensure that data belonging to different customers is compartmentalized and never mixed, maintaining the privacy and integrity of each customer's information.

Multi-Tenant Systems: Despite running multi-tenant systems, data isolation is rigorously maintained to prevent any crossover or co-mingling of data between different customers.

## Encryption in Transit and Backup

All data transferred within our systems is encrypted to ensure the confidentiality and security of information during transmission. Additionally, all backups, including point-in-time backups, are encrypted, safeguarding the integrity of backed-up data. In relevant contexts the data is encrypted also at rest.

## Data Loss Prevention Measures

Data loss prevention strategies at Liana Technologies are meticulously tailored based on the value and business impact of the systems in place. We employ various methods to mitigate data loss risks, ensuring the resilience and availability of data.The stack of methods for any use case is always determined based on the business needs:

- Backup Redundancy. Regular backups (minimum daily) are conducted across all systems to prevent data loss in case of unexpected incidents or system failures. The backups are physically isolated from other systems.

- Duplicated Databases. Duplication of databases serves as an additional layer of protection, enhancing redundancy and minimizing the risk of data loss.

- Point in time backups. In some cases we also do point-in-time backups to ensure swift recovery.

These comprehensive measures are aimed at fortifying the security and integrity of data within our systems, ensuring continuous availability and protection against potential data loss scenarios.

# Security Monitoring and Auditing

## System Availability Monitoring and Logging

At Liana Technologies, we prioritize the continuous availability of our systems. We employ robust monitoring mechanisms to track system performance, availability, and security-related activities:

- Availability Monitoring. Our systems are continuously monitored to ensure high availability and prompt identification of potential issues.

- Logging Practices. We log all relevant activities within our systems to maintain an audit trail, capturing vital information for analysis and security incident investigations. However, we do not log anything for which we do not have a predetermined purpose.

## Isolated Management of Logs, Metrics, and Alarms

To uphold the integrity of our monitoring practices, logs, metrics, and alarms are managed in an isolated system separate from the systems they monitor. This segregation ensures that monitoring data remains secure and tamper-resistant.

## Security Audits and Assessments

We conduct regular security audits and assessments, evaluating our systems, processes, and controls to ensure compliance with established security standards and to identify areas for improvement.

# Business Continuity and Disaster Recovery

At Liana Technologies, our commitment to information security, regulatory compliance, access control, data protection, monitoring, and auditing culminates in a robust business continuity and disaster recovery framework.

## Continuous Support and Availability

We ensure continuous support and availability of our systems through a dedicated 24/7/365 on-call team. This team is readily available to address any critical issues, ensuring swift resolution and minimal disruption to our services.

## Automated Software Deployment for Business Continuity

Business continuity is guaranteed through our automated infrastructure provisioning and software deployment processes. These sophisticated systems enable us to recreate environments swiftly in case of catastrophic failures.

**Data Recovery from Isolated Backups.** In the event of catastrophic failures, our deployment processes leverage data from physically isolated backups. These backups serve as a reliable source, allowing us to restore systems efficiently.

# Ensuring Resilience and Recovery

The culmination of our security measures, combined with our commitment to 24/7 availability and automated deployment processes, guarantees a robust business continuity and disaster recovery capability. This allows us to maintain service integrity and swiftly recover from any unforeseen incidents, ensuring our customer’s trust and uninterrupted service delivery.

# Closing Statement

At Liana Technologies, the security and integrity of our systems and your data are paramount. This comprehensive information security guidelines document represents our steadfast commitment to transparency, compliance, and proactive measures in safeguarding your valuable information.

While this document serves as an overview of our security practices and protocols, we understand the importance of tailored information specific to your needs. We welcome and encourage inquiries for additional information, deeper insights, or clarifications on any aspect discussed herein.

Thank you for entrusting Liana Technologies with your business needs. We look forward to continuing our partnership in ensuring the security and success of your endeavors.