

Information Security Management Policy

| | |
|---------------------|---|
| Author | Marc Benson - Signagelive CTO |
| ISMS Classification | Public |
| v1.0 | Marc Benson - July 2021 - Document Created |
| | Marc Benson - October 2022 - Document Review |
| | Marc Benson - October 2023 - Document Review |
| v2.0 | Marc Benson - September 2024 - Document Created |
| | Marc Benson - September 2025 - Document Review |

1. Introduction

This Information Security Management Policy outlines the framework for managing information security within Signagelive, a Software as a Service (SaaS) provider. The objective of this policy is to protect the confidentiality, integrity, and availability of information assets while ensuring compliance with relevant legal and regulatory requirements.

2. Scope

This policy applies to all employees, contractors, and third-party service providers who have access to Signagelive's information systems and data. It covers all information assets related to the development, maintenance, and operation of our SaaS products.

3. Objectives

- Protection of all data assets held, processed and managed by Signagelive
- Satisfaction of all client requirements within defined SLA and project specific expectations
- Continued resilience of all solutions deployed within our information processing environments
- Maintain a risk-managed and controlled supply chain capable of meeting our security expectations and their SLA offerings
- Continued accessibility to Signagelive services
- Prevention of cyber security impacts and attacks

4. Governance

The ISMS will be governed by an internal ISO team led by an appointed Information Security Officer. This team will be responsible for:

- Developing and maintaining Information Security Management System policies and procedures.
- Conducting regular risk assessments.

- Ensuring compliance with ISO 27001 requirements.
- Reporting on Information Security Management System performance to senior management.

5. Risk Management

A comprehensive risk assessment will be conducted annually to identify potential threats to information assets. The risk management process will include:

- Identifying assets and their vulnerabilities.
- Evaluating risks based on likelihood and impact.
- Implementing appropriate controls to mitigate identified risks.

6. Information Security Controls

The following controls will be implemented as part of the Information Security Management System :

- **Organizational Controls:** Policies and procedures that define roles and responsibilities related to information security.
- **People Controls:** Employee training programs to raise awareness about information security threats and best practices.
- **Physical Controls:** Measures to secure physical access to information systems and data centers.
- **Technological Controls:** Use of encryption, access controls, and monitoring systems to protect data from unauthorized access.

7. Incident Management

Signagelive will establish an incident response plan that outlines procedures for detecting, reporting, and responding to security incidents. Employees will be trained on how to recognize potential security breaches and report them promptly.

8. Compliance

The Information Security Management System will ensure compliance with applicable laws, regulations, and standards, including but not limited to:

- ISO 27001
- General Data Protection Regulation (GDPR)

9. Monitoring and Review

The effectiveness of the Information Security Management System will be monitored through regular audits and assessments. The policy will be reviewed annually or as needed in response to significant changes in the organization or its environment.

10. Policy Approval

| | |
|------|-------------|
| Name | Marc Benson |
|------|-------------|

| | |
|-----------|-------------|
| Date | 2025-09-10 |
| Signature | Marc Benson |

It is mandatory for all employees and stakeholders to adhere to this policy as part of their responsibilities within Signagelive.

Audit trail

Details

| | |
|------------------|---|
| FILE NAME | ISMS Policy - Sept 2024 - 10/09/2025, 09:40 |
| STATUS | <div><div></div>Signed</div> |
| STATUS TIMESTAMP | 2025/09/10 08:41:30 UTC |

Activity

| | | |
|--|---|----------------------------|
| <div><div></div><div>SENT</div></div> | marc@signagelive.com sent a signature request to: <ul style="list-style-type: none">Marc Benson (marc@signagelive.com) | 2025/09/10 08:40:34 UTC |
| <div><div></div><div>SIGNED</div></div> | Signed by Marc Benson (marc@signagelive.com) | 2025/09/10 08:41:30 UTC |
| <div><div></div><div>COMPLETED</div></div> | This document has been signed by all signers and is complete | 2025/09/10 08:41:30 UTC |

The email address indicated above for each signer may be associated with a Google Account, and may either be the primary email address or secondary email address associated with that account.