INFORMATION SECURITY POLICY

Document Version	24.1.01
Date	December 20, 2024

TABLE OF CONTENTS

1. INTRODUCTION

An information security policy is the cornerstone of an information security program. As such, this information security policy reflects SMA Technologies objectives for security and the agreed upon management strategy for securing information and continual improvement. SMA Technologies information security policy is its foundation for protecting SMA Technologies information, systems, and people, as well as its intellectual property, customer and partner relationships, company brand, and investor value.

2. PURPOSE

The purpose of the Information Security Policy is to set forth the underlying tenets, framework, and reasoning for SMA Technologies Information Security Management System (ISMS) in accordance with the requirements of ISO standard ISO/IEC 27001 and SOC 2

3. INFORMATION SECURITY POLICY STATEMENT

It is the policy of SMA Technologies to protect the confidentiality, integrity, and availability (CIA) of the information held, in any form.

This Information Security Policy is supported and complemented by other policies, procedures, standards, and other remaining ISMS documentation.

SMA Technologies ISMS supports the following objectives:

- Demonstrate management commitment to, and support for, information security;
- Establish directives and principles for action with regards to information security;
- Ensure alignment with the company's business continuity requirements;
- Ensure alignment with client requirements and contractual security obligations;
- Ensure alignment with applicable legal and regulatory requirements;
- Ensure alignment with applicable privacy requirements; and
- Ensure alignment of the ISMS with the enterprise risk management approach.

The risk management approach for the ISMS shall be aligned with the organization's strategic risk management context.

SMA Technologies risk assessment criteria are derived from the ISO 27005 risk assessment methodology. SMA Technologies assesses risks to information assets qualitatively by estimating the impact and likelihood of information security events within the organization.

The ISMS Manager is responsible for maintaining this Information Security Policy, supporting its objectives, and advising on its implementation.

Continual improvement needs will be determined by various methods. The ISMS Manager is responsible for ensuring the improvement activity is operationalized, based on factors such as alignment with business and security objectives, needed resources, budget and technological feasibility, the improvement aligns with SMA Technologies security roadmap and is approved by either the ISMS Steering Committee or the Executive Leadership Team, as applicable.

Conformance at every level to the Information Security Policy and all remaining ISMS policies, standards, and procedures, is mandatory.

The Information Security Policy must be reviewed at least annually.

4. OWNERSHIP AND REVIEW

This policy is owned by the ISMS Manager.

This policy shall be reviewed on an annual basis.

Changes to this document shall be in accordance with the ***ISMS Document and Records Control Standard.***

4.1. CONTACT INFORMATION

ISMS Manager/Director of Security
(281)446-5000
ISMS@SMAtechnologies.com

4.2. DOCUMENT RACI

Responsible	Assigned to do the work	ISMS Manager
Accountable	Final decision, ultimately answerable	Executive Leadership Team
Consulted	Consulted BEFORE an action or decision is taken (proactive)	ISMS Steering Committee
Informed	Informed AFTER a decision or action has been taken (reactive)	Named Participants in this document Other parties affected by the change