ACCEPTABLE USE POLICY

Document Version	23.1.02
Date	November 2, 2023

TABLE OF CONTENTS

1. INTRODUCTION

1.1. PURPOSE

SMA Technologies intends to make information resources available to employees and authorized users with the expectation that these resources will support a valid business use. Each resource introduces inherent risks. In response to those risks SMA Technologies creates and maintains this Acceptable Use Policy governing the usage of SMA Technologies information resources. This policy provides management support for proper conduct principles, and unambiguously demonstrates, to stakeholders, the management commitment to a healthy and productive environment. This policy is supported by People Ops.

1.2. BACKGROUND

Acceptable use of corporate assets requires sensitivity to the SMA Technologies environment, responsible stewardship of assets that the stakeholders have entrusted to SMA Technologies, and compliance with all legal and ethical responsibilities.

2. SCOPE

2.1. USERS

This policy will affect all users of SMA Technologies information resources regardless of the information format.

2.2. SYSTEMS

This policy will affect various systems, dependent on the nature and source of the usage under question.

3. ENVIRONMENT

Objective: To establish an environment to optimize the SMA Technologies mission.

A. All entities granted access to SMA Technologies information assets shall be required to complete a non-disclosure agreement (NDA) and or a confidentiality agreement to uphold information confidentiality. Failure to complete the agreement shall result in denial of access.

B. The ability to access information or content, whether internal or external, does not imply any consent regarding the use of such assets.

C. The act of downloading/uploading, creating and/or displaying items of a pornographic or prurient sexual nature creates an uncomfortable or hostile environment, and such activity is prohibited.

D. The act of downloading /uploading, creating and/or displaying items of a racist or sexist nature, or negatively targeting any identifiable group, can create an uncomfortable or hostile environment and such activity is prohibited.

E. The act of downloading /uploading, creating and/or displaying items that elicit an uncomfortable response, or are deemed inappropriate, is prohibited. Management reserves the right to determine what is or is not appropriate.

F. There is no guarantee of privacy while using SMA Technologies infrastructure. Information created or stored on SMA Technologies equipment is considered the intellectual property of SMA Technologies. Management reserves the right to monitor workstation activity and examine incidents on any equipment at any time as allowed by local, federal, or international law.

4. STEWARDSHIP

Objective: Retain stakeholder trust by demonstrating responsible stewardship toward corporate assets.

A. Downloading of large or streaming files requires excessive bandwidth. To ensure availability of SMA Technologies information resources for all business needs, care should be taken regarding such activities.

B. Attempts to intentionally damage or hinder SMA Technologies information resources, such as the introduction of viruses, worms, or other forms of malicious software is prohibited.

C. Uncontrolled software, freely available on the Internet or via other sources, often harbors hidden malicious intent and may result in the inadvertent introduction of viruses, worms, Trojans, and other forms of malicious code. Introduction of ANY software not approved by the Information Security Program is prohibited.

D. Employees, in the course of their employment with SMA Technologies, may be exposed to protected information and are bound by the requirements of the SMA Technologies ***Information Classification and Handling Standard***. Protection requirements specifically address the protection of removable storage media such as USB flash drives, external disk drives, or memory cards.

E. Employees, in the course of their employment with SMA Technologies, may be issued mobile computing devices such as laptop computers and tablets and are therefore bound by the requirements of the SMA Technologies ***Information Classification and Handling Standard*** and any other policies or standards applicable to the use of mobile devices. Protection requirements specifically address the concerns of sensitive data resident on portable computing devices at home, in airports, airplanes, automobiles, hotels or other areas with marginally controlled physical security.

F. Care must be taken to ensure the physical security of mobile computing devices. For those employees working in the physical SMA offices, at the end of the workday, either take the mobile computing device home or lock it in a drawer or cabinet. Mobile computing devices outside of the office must not be left unattended in plain sight for even short periods of time. Mobile computing devices must not be left in vehicles overnight, even if those vehicles are locked.

G. Usage of SMA Technologies information resources is intended for its business purposes.

H. Information Security is everyone's responsibility, and it is every individual user's responsibility to report any real or suspected violation of SMA Technologies policies and/or standards.

5. COMPLIANCE

Objective: To comply with all legal and ethical responsibilities

A. Unauthorized reproduction of copyrighted works, such as software and documentation, is an infringement of intellectual property laws, and is prohibited. Unauthorized duplication of copyrighted material may subject users and/or the company to both civil and criminal penalties under the United States Copyright Act or other applicable international copyright regulations.

B. Employees may duplicate any SMA Technologies developed licenses, software, or related documentation for use either on the company's premises, or elsewhere, as required to deliver contracted services. Employees may provide SMA Technologies licensed software to third parties including contractors, customers, and others whenever there is a non-disclosure agreement in place. During the pre-sale, evaluation period, the software license key shall be time-restricted.

C. Employees may not duplicate any third-party developed licenses, software, or related documentation for use either on the company's premises, or elsewhere, unless such duplication is expressly authorized by the End User Licensing Agreement or the licensing agreement with the publisher. Employees must not provide licensed, third party software to any outsiders including contractors, customers, or others.

D. Workstations shall be cleared of sensitive information and secured while unattended if the employee is away from their desk for an extended period of time.

E. For those employees working in the physical SMA offices, desks and work surfaces shall be cleared of sensitive information while unattended for an extended period of time and at the end of the work shift prior to leaving.

F. For those employees working in the physical SMA offices, laptops shall be shut down or hibernated and locked up in a cabinet or taken home at the end of the work shift.

G. Printers and other devices which could disclose sensitive information in printed form shall be cleared of such information in a timely manner.

H. Use of SMA Technologies communication media, such as email and instant messaging, to send threatening or harassing communications is prohibited, and may result in investigation by relevant law enforcement authorities.

I. Certain employee or customer records, such as social security numbers, are protected against unauthorized access. Disclosure, either accidental or intentional, may subject the responsible party to the full measure of recourse.

J. Any attempt to circumvent access controls, or "hacking," regardless of intent, is a violation of company policy and may be subject to SMA Technologies Progressive Disciplinary Process. Any such attempts may also be in violation of the federal Computer Fraud and Abuse Act, as well as applicable international, state, and local law, and may subject the violator to prosecution.

K. Utilization of SMA Technologies information resources for personal gain, such as gambling or self-marketing, is unethical and hence prohibited.

L. Casual and limited personal use of SMA Technologies information resources is allowed on a non-interfering basis. Sending and receiving an occasional personal email, and "break time" web surfing may be considered examples of casual personal use.

M. Unless the application prohibits multiple accounts, user passwords shall not be disclosed to or shared with others. Sharing user accounts and passwords hinders the ability to hold users accountable for their activities and may result in false accusations against the legitimate account holder. Account sharing may also result in identity theft. Sharing of accounts, passwords and other user access information must be strictly controlled when individual accounts are not provided. Otherwise, sharing of accounts, passwords and other user access information is strictly prohibited.

N. Storage of source code, customer information, and other sensitive or confidential information shall not be transferred or stored on non-SMA Technologies devices.

O. USB ports on laptops are restricted by default, meaning that any unapproved USB device that is plugged into a laptop will be denied and disconnected. If an employee needs an exemption, they will have to document the device that they want to have approved, providing a valid business reason and have their manager approve it in writing. Then, using that email chain, a ticket should be created in the IT ticketing system for processing.

6. SOCIAL NETWORKING USE

Objective: To limit business risk exposure related to the use of social networking

A. Access from within the SMA Technologies network to social networking services and sites not specifically intended to support SMA Technologies business goals shall be prohibited.

B. The personal use of any chat or streaming media service shall not be permitted without management approval.

C. Social networking posts must conform to all relevant requirements of both this policy and the information security program.

D. Employees shall not claim to represent SMA Technologies in social network postings or messages unless specifically authorized to do so by management.

E. Employees shall not defame or otherwise discredit the products or services of the company, their partners/resellers, affiliates, customers, vendors, or competitors.

F. Employees shall not defame or otherwise discredit by way of social media posts SMA Technologies logo, trademark, proprietary graphics or photographs of the company's premises, personnel, or products without explicit management approval.

G. Postings, whether business-related or personal, must not contain information that SMA Technologies considers derogatory or damaging to the company's reputation and goodwill. Any such posts, even those made anonymously, are subject to investigation and appropriate remedial action by the company.

H. Violations of the above rules may result in both disciplinary action (recourse) and remedies in law.

7. RECOURSE

Objective: To ensure management of policy violations

Compliance with this ***Acceptable Use Policy*** is a condition of resource usage as well as a means for enforcement. Users shall have no expectation of privacy while using SMA Technologies information resources. SMA Technologies reserves the right to monitor usage of SMA Technologies information resources and to take relevant disciplinary action based upon inappropriate use. Recourse is managed by People Ops.

8. 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.***

9. CONTACT INFORMATION

ISMS Steering Committee
(281)446-5000
ISMS@SMAtechnologies.com

10. DOCUMENT RACI

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