INCIDENT RESPONSE POLICY & PROCEDURE

Document Version	22.2.01
Date	October 27, 2022

TABLE OF CONTENTS

1 INTRODUCTION

1.1 PURPOSE

Incident response capabilities are used to monitor for security incidents, determine the magnitude of the threat presented by these incidents, and to respond to these incidents. Without an incident response capability, the potential exists that, if a security incident occurs, it will go unnoticed, and the magnitude of harm associated with the incident will be significantly greater than if the incident were noted and corrected.

SMA Technologies is committed to protecting the privacy and security of its protected data. If an incident is identified as a potential breach of its protected information, SMA Technologies will investigate the suspected breach and take appropriate corrective and remedial action.

1.1.1 OBJECTIVE

The primary goals of incident response are to determine the cause and effect of incidents, including any sanctions that may be appropriate and any new preventive measures that may need to be implemented, as well as to restore the affected infrastructure to an operational state in a timely manner.

SMA Technologies recognizes that all Incidents also constitute an Information Security Event (Event). However, by definition, not all Events will result in an Incident. An Event will be reported as such whenever something happens that is generally considered unusual, whether planned or unplanned, but does not result in an interruption of service or systems or any other compromise which would be considered an Incident.

This Incident Response Policy and applicable addenda are intended to create an incident response program with the authority to create an incident response team and to establish standardized procedures for responding to security-related events affecting SMA Technologies information technology resources. A standardized approach to handling security-related events will facilitate thorough information gathering and reporting; and allow for timely remediation.

Information is a critical asset of the company, and accurate, timely, relevant, and properly protected information is essential to the company’s business. To ensure that information is properly handled, all access to, and use and processing of, SMA Technologies information must be consistent with SMA Technologies Information Systems related policies and standards.

1.2 AUDIENCE

The Incident Response Policy applies equally to all individuals that use any information resources.

1.3 SCOPE

This policy applies to all information systems, data, information system components and users of SMA Technologies information technology resources and governs the company's general response, documentation, and reporting of security incidents affecting those resources. Information technology resources include any electronic device or system that is used to create, store, retrieve or transmit information of any kind and in any form on behalf of the Company.

This includes but is not strictly limited to:

- Servers and other devices that provide centralized computing capabilities
- Devices or applications that provide storage capabilities
- Desktops, laptops, and other devices such as smartphones and tablets, that provide distributed computing capabilities
- Routers, switches, and other devices that provide network capabilities
- Firewalls, IDS sensors and other devices that provide dedicated security capabilities
- Databases and files contained in above systems
- Restricted and Confidential data contained in the above systems
- Restricted and Confidential information, paper-based

2 POLICY

SMA Technologies defines an Information Security Incident ("Incident") as any activity that harms, compromises, or threatens to harm or compromise, in whole or in part, any aspect of SMA Technologies information technology resources or restricted and sensitive information. This includes, by way of example, acts or omissions that cause an interruption of service; inhibition of functioning systems; unauthorized changes to hardware, firmware, software, or data; unauthorized exposure, change or deletion or destruction of information.

While every effort has been made to have this policy reflect the state of technology as of the date of its adoption, technological developments nonetheless may outstrip the literal text of certain aspects of this policy. In view of the foregoing, SMA Technologies expects that employees will be sensitive to the underlying spirit and intent of this policy and will look to the goals this policy is intended to achieve. Employees should not attempt to do indirectly what this policy prohibits directly, and they should not employ means to defeat the goals that this policy is intended to achieve, even though these means may not have been mentioned in this policy.

The provisions of this policy continue, where applicable, following the departure of company personnel from the company.

Any suspected or known violations of this policy must be reported immediately to the ISMS Manager or the ISMS Steering Committee so that the security Event or Incident can be documented, investigated, contained, and remediated in a timely manner.

3 RESPONSIBLE PARTIES

The Incident Commander has the responsibility, as necessary, for establishing an Incident Response Team that will be responsible for responding to Incidents. This includes interdiction and remediation, as well as conducting all security related investigations, to gather and analyze the incident data, determine the impact of the Incident, limit the damage to the company, restore normal services and system integrity, and help prevent future Incidents.

Core members have been assembled for the Incident Response Team due to their job function within SMA Technologies. Depending on the type and severity of the Incident, key representatives from specific departments (e.g., Legal, People Ops, Security, etc.) will be required to act as members of the Incident Response Team. The Incident Response Team has responsibility for determining the trigger points of involvement by other SMA Technologies business units and functional departments based on the specific requirements outlined by those groups, and involving the applicable groups based on those requirements.

4 PROCEDURE

This plan governs all types of security incidents.

A.16.1 Management of information security incidents and improvements	
Control Statements	**Annex A Reference**
SMA Technologies has established responsibilities and procedures to ensure that events are reviewed quickly and, if an incident, there is a quick and orderly response to incidents regarding information security.	A.16.1.1 Responsibilities and procedures
It is SMA Technologies policy that information security events should be reported through the appropriate management channels as quickly as possible, in accordance with the representatives shown above. Should a SMA Technologies worker observe or be aware of an event, and management representation is in question, that SMA Technologies worker should immediately contact the ISMS Steering Committee or People Ops to report the event.	A.16.1.2 Reporting of security incidents

A.16.1 Management of information security incidents and improvements	
Any SMA Technologies employee, contractor or vendor may report an incident, event, activity, or concern to any member of the ISMS Steering Committee. Business Technology & Information Services may also identify an incident through its proactive monitoring of SMA Technologies information technology resources. Once reported, the activity shall be turned over to the Incident Response Team for evaluation and response.	A.16.1.3 Reporting information security weaknesses

4.1 IDENTIFICATION AND CLASSIFICATION

The type of security incident and the severity should be classified based on best known information at the time and revised as new information becomes known.

4.1.1 TYPE OF EVENT

Security events may take, but are not limited to, these forms:

- A phishing campaign for password resets
- A phishing campaign targeting direct deposit changes
- A phishing campaign targeting fraudulent wire transfers
- A violation of security policies
- A breach of information
- Attempts to gain unauthorized access
- Excessive port scans
- A denial of service attack
- Malicious code outbreak
- Unauthorized use or modification of resources
- Defamation of brand (hacking and/or defaces SMA Technologies website or social media accounts)
- Civil unrest
- Theft

Once an investigation has been conducted, an Event may be escalated to an Incident if the Event meets the definition of an Incident as stated in Section 2 – Policy.

4.1.2 THREAT LEVEL OF AN INCIDENT

Once an Event is categorized as an Incident, the Incident Response Team shall establish an incident classification matrix to focus and tailor the response to the Incident and will involve the appropriate team participants. This will also better allow the Incident Response Team to prioritize the Incident. This classification matrix shall indicate which authorities at SMA Technologies to involve and which procedure is applicable for each class of Incident.

An incident requires an assigning of criticality based on what individuals, including appropriate law enforcement authorities (e.g., local police or FBI), need to be involved and the severity of the incident. Based off the extent of potential damage to SMA Technologies and its associates, a ranking may be elevated without meeting the below criteria.

Information security incidents, including but not limited to cyber-security incidents, will be rated per the following severities:

Severity	Description
Critical	Defined as a large exposure of information, assets, or services that negatively impacts SMA Technologies in a severe manner as an organization. Critical rankings would be issued in severe circumstances and require many members within the organization to assist. Critical rankings may be escalated to the appropriate law enforcement authorities as referenced in the ***SMA Business Continuity Plan***.
High	Classified as an incident that negatively impacts business or loss of confidentiality, integrity of availability of systems. Other high classifications could be focused and targeted attempts of attack or large-scale virus outbreaks. High rankings may be escalated to the appropriate law enforcement authorities as referenced in the ***SMA Business Continuity Plan***.
Medium	Incidents that require quick response to combat a specific threat that does not directly cause large damages towards the organization but can potentially elevate if left untreated. Medium rankings may be escalated to the appropriate law enforcement authorities as referenced in the ***SMA Business Continuity Plan***.
Low	Incidents that do not damage SMA Technologies assets; however, require further investigation to ensure incident is handled in an acceptable manner. Low rankings will likely not be escalated any further.

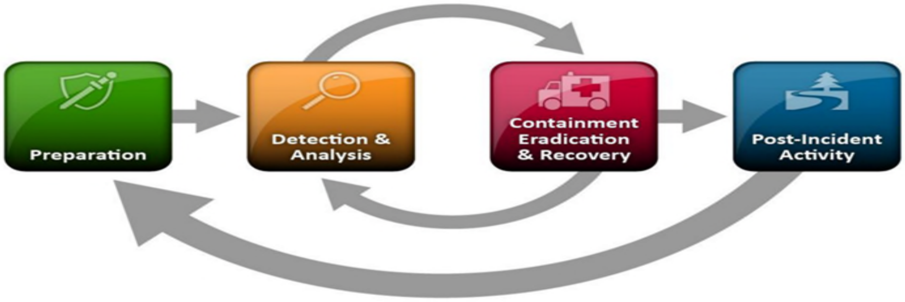
4.2 IMMEDIATE TRIAGE AND RESPONSE

After receiving a report of an Event, activity or concern, the Incident Commander or the Incident Response Team shall assess its veracity to determine whether the Event constitutes an Incident. If it is confirmed to be an Incident, then the Incident Commander or designated official will categorize the Incident and a priority classification shall be determined.

4.3 INCIDENT RESPONSE STEPS

4.3.1 SUMMARY

SMA Technologies models the IR lifecycle based on NIST SP 800-61 guidance which divides the process into four phases.



Preparation:

Actions taken to reduce the likelihood of a security incident and to ensure that the organization is in a defensible position.

Detection & Analysis:

Efforts to identify potential security incidents and understand their impact to the organization as well as efforts to maintain situational awareness around various threats.

Containment, Eradication & Recovery:

Active measures taken to limit the damage of a confirmed security incident and to return the environment to a secure state.

Post-Incident Activity:

After action reviews conducted to gather lessons learned and to improve the organization’s incident response capabilities.

4.3.2 DETECTION

The most difficult task in this procedure can be the identification of a security incident amidst the general noise of daily activity. Reports of an Event can come from any number of sources such as employees, vendors, customers, partners, or facility management. The Incident Commander, based on the information provided, determines if an Incident has occurred and proceeds to the assessment phase, assembling additional team members as needed.

4.3.3 ANALYSIS

A.16.1 Management of information security incidents and improvements	
Control Statements	**Annex A Reference**
Not every reported event, upon assessment, is deemed to be an information security incident. The Incident Response Team and any business area impacted will perform the assessment and classify the relevant events as information security incidents.	A.16.1.4 Assessment of and decision on information security events

Once an Event meets the criteria of an Incident, the Incident Response Team shall use a formal and systematic process for responding to the Incident. This process shall be comprised of several phases from initial response preparation through post-incident analysis. The Incident Response Team will work with others as appropriate and take the appropriate steps to investigate, gather evidence, analyze, contain, eradicate, and remediate the Incident. The Incident Response Team is responsible for all documentation throughout the Incident response process.

The Incident Response Team shall determine the impact and magnitude of the incident. It is important not to rush to action, such as turning off a computer, as this may cause a loss of data or evidence needed for a later investigation. Factors to consider are:

- How many computers are affected?
- Is secret information involved?
- What is the entry point of the incident?
- What is the potential damage?
- What is the estimated recovery time?
- What external agencies (e.g., law enforcement authorities, clients) need to be notified?
- What additional resources may be required?
- Was any customer data compromised?

As warranted by the Incident Response Team's assessment, proper notification will be delivered to upper levels of management, customers, law enforcement authorities, and any vendors/services that may be impacted. If a breach of customer PII has occurred, breach notification will comply with all legal requirements. If a breach occurred of PII data belonging to a customer, the customer will be notified of the breach with the intent to formalize a joint response to the customers affected.

4.3.4 CONTAINMENT

A.16.1 Management of information security incidents and improvements	
Control Statements	**Annex A Reference**
SMA Technologies includes response to incidents by type of information security incident. Overall, the Incident Response Team is the decision-maker regarding (1) whether the incident requires escalation internally to the Executive Leadership Team or externally to law enforcement authorities before response or (2) what method of response is to be used.	A.16.1.5 Response to information security incidents

To regain control and limit damage, the Incident Response Team may choose to disconnect the compromised system from the rest of the network. However, consideration must be given to the affect this may have on the business functions. The Incident Response Team may also change passwords to prevent installation of Trojan programs that would provide backdoor access.

For non-IT incidents, containment may include involvement of law enforcement authorities, replacement of assets and/or worker education.

4.3.5 ERADICATION AND RECOVERY

Once an Event has been classified as an Incident, additional investigation should be performed to determine the cause of the incident. This may include reviewing logs from multiple systems. Care should be taken when using administrative tools on the compromised system as they may have been compromised as well to inflict further damage. Consider using a separate set of administrative tools.

After the investigation, a clean operating system should be loaded and hardened with the latest patches, disabling unnecessary services, installing anti-virus software, and applying any additional requirements to the security policy. After business functionality has been restored, the system should be monitored in a test environment before it is placed back into production. Additional monitoring should be added in the production environment to detect a return by the attacker.

4.3.6 POST-INCIDENT ACTIVITY

A.16.1 Management of information security incidents and improvements	
Control Statements	**Annex A Reference**
Upon completion and remediation of a specific incident, a review process will be initiated to document the current incident response program and how effective a specific event was handled as well as preventive measures to ensure the same incident does not occur again. The Incident Commander also determines what, if any, additional steps (e.g., employee training) will help in mitigating the risk of similar future Events.	A.16.1.6 Learning from information security incidents

Finally, the Incident Response Team shall perform a detailed analysis to determine how the incident occurred and how it can be prevented. In addition, if legal action is required, outside investigators may be required to ensure that evidence integrity is preserved for acceptance in court.

A.16.1 Management of information security incidents and improvements	
Control Statements	**Annex A Reference**
SMA Technologies has taken steps to ensure that evidentiary records are defined. Procedures are in place for identification, collection, acquisition, and preservation of any information that may serve as evidence. The Incident Response Team shall ensure that all Events and Incidents are appropriately logged and archived. Incident Response Team representatives shall be responsible for communicating the Incident to appropriate personnel in a timely manner and maintaining contact, for update and instruction, for the duration of the Incident Summary reporting on information security incidents shall be given to the Executive Governance and ISMS Steering Committees monthly. The Incident Response Team will use standard internal procedures to log and track Incidents and is responsible for maintaining these records.	A.16.1.7 Collection of evidence

Documentation should be filed with the incident ticket. Along with a summary for management, the documentation may include:

- System events with audit records
- Actions taken including the time performed
- Notes from external conversations including person, time, and content
- A description of the exact sequence of events
- Method of discovery
- Preventative measures added
- Further recommendations

The overall goal for documentation is to improve the systems and procedures, including this incident response procedure.

4.3.7 PREVENTION

To prevent Events and subsequent Incidents, SMA Technologies regularly monitors and scans its own network for anomalies and continues to develop clear protection procedures for the configuration of its Information Technology Resources.

The Incident Response Team shall ensure that Incidents are properly recorded in its system of record. Following the closure of an Incident, security will conduct a post-Incident review to capture lessons learned and track identified areas of improvement.

4.4 SUSPICOUS ACTIVITY NOTIFICATION

Any individual should report suspicious activity to the security team via email to ISMS@SMAtechnologies.com and Business Technology & Information Services at BTIS@SMAtechnologies.com.

The Incident Response Team will review the potential incident; and in the event of potentially critical incidents, the Incident Response Team will alert the ISMS Steering Committee and the Executive Leadership Team as required.

For confirmed data breach incidents involving customer data, the Incident Response Team will work with the Executive Leadership Team to notify the respective customer's security team in a timely manner (within 24 hours of a confirmed incident, barring extreme circumstance).

5 COMPLIANCE

Compliance with this policy is vital to the business success of SMA Technologies and the information security management program. As a SMA Technologies employee, it is your responsibility to:

- Learn and understand the requirements of this policy
- Apply the requirements of this policy to your job responsibilities and activities

- Comply with the requirements of this policy as outlined in Section 2, above
- Cooperate fully in any audit or investigation related to any suspected Event or violation of this policy
- Report any violation of this policy to the ISMS Steering Committee
- If you are manager or supervisor, you have additional responsibilities including:
    - Making certain that associates know and understand this policy and the appropriate application of it
    - Taking affirmative steps to prevent violations of this policy
    - Establishing proactive methods to determine if violations of this policy have occurred
    - Assuring that any associate who reports a suspected violation of this policy is protected from retaliation

6 DISCIPLINARY ACTIONS

Violation of this policy may result in disciplinary action up to and including termination for employees including temporaries; please refer to the Progressive Disciplinary Policy for each respective location.

7 OWNERSHIP AND REVIEW

This Incident Response Policy is owned by the ISMS Manager.

This Incident Response Policy shall be reviewed on an annual basis.

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

7.1 CONTACT INFORMATION

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

7.2 DOCUMENT RACI

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