Information Security Incident Management Policy

Policy Title	**Information Security Incident Management Policy** **Part of Information Security Policy Framework**
Responsible Party	Chief Security Officer ("CSO")
Endorsed by	Information Security Policy Committee
Contact	Chief Security Officer, Stuart Zimmerman; (918) 858-6684
Effective Date	June 1, 2015
Last Update	April 1, 2022

I. Policy Statement

TMA Systems possesses information corporately, for their clients, and for their business associates that is sensitive and valuable. Because the Company takes information security very seriously, prompt action must be taken in the event of any actual or suspected breaches of information security or confidentiality. Prompt action will avoid, or minimize the risk of harm to the Company, clients, partners, or their respective employees. In addition, prompt action will minimize: damage to operations, financial losses, legal exposure and damage to the organization's reputation.

The Company requires all employees to diligently protect information as appropriate for its sensitivity level and report suspected information breaches promptly so appropriate action can be taken and harm can be minimized.

Failure to comply with this policy may subject you to disciplinary measures up to and including termination and other legal remedies.

II. Policy

- **Purpose of Policy**
- **What is an Information Security Incident?**
- **What and Who the Policy Applies to**
- **Where the Policy Applies**
- **Investigation and Potential Notifications Related to a Breach**
- **Responsibility for Creating a Culture of Information Security**

Purpose of Policy

The goal of the policy is to support the prompt and consistent management of information security incidents in order to minimize any harm to the Company, clients, partners, or their respective employees.

To this end all individuals associated with the company, both employees and consultants who utilize TMA's IT and digital resources need to:

- Understand their roles in reporting and managing suspected incidents
- Report actual or suspected information security incidents promptly by escalating to the correct individuals
- Accurately record the incident to assist in the investigation and development of actions to strengthen information security controls

What is an Information Security Incident?

An information security incident is any event that has the potential of affecting the confidentiality, integrity, or availability of Company information in any format. Examples of information security incidents can include but are not limited to:

- The disclosure of confidential information to unauthorized individuals
- Loss or theft of paper records, data or equipment such as tablets, laptops and smartphones on which data is stored
- Inappropriate access controls allowing unauthorized use of information
- Suspected breach of the Corporate and communications use policy
- Attempts to gain unauthorized access to computer systems, e, g hacking
- Records altered or deleted without authorization by the data "owner"
- Virus or other security attack on IT equipment systems or networks
- "Blagging" offense where information is obtained by deception
- Breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing confidential information left unlocked in an accessible area
- Leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information
- Covert or unauthorized recording of meetings and presentations

What and Who the Policy Applies to

This policy applies to the following:

- All information created or received by the Company in any format, whether used in the workplace, stored on portable devices or media, transported from workplace physically or electronically or accessed remotely
- All individuals associated with the Company, this includes: employees, consultants, or contractors working for or on behalf of the Company and any other person permitted to have access to TMA's IT and digital resources
- All Company IT systems managed by the Company or IT systems which Company information is held or processed

The parties that this policy applies to:

The policy applies to all users of Company information. Users include all employees, consultants, suppliers, or contractors working for or on behalf of the Company and any other person permitted to have access to TMA's IT and digital resources including visitors.

Where the Policy Applies

This policy applies to all locations from which Company information is accessed. This includes: TMA's Corporate offices, remote access from client sites and home use.

Lines of Responsibility

- All users who are given access to TMA's IT and digital resources are responsible for reporting any actual or potential breach of information security promptly in line with the defined incident management procedures
- The Chief Executive Officer ("CEO") has ultimate responsibility for Information Security. In the event of a suspected incident involving IT facilities, the CEO is the only person who can authorize the monitoring of a user's IT account, including: use of computers, use of the Internet, and email when investigating allegations of illegal activity, improper activity, or relevant breaches of information security. In addition, the CEO is only person who can, when necessary, report these to relevant legal authorities. The CEO will work in conjunction with the CSO on these matters.
- The Chief Security Officer ("CSO") and the Information Guardians (as defined in the Information Security Policy), are responsible for identifying specific categories within the circle of their responsibility that are considered "Confidential" and "Highly Confidential" (as defined in the Information Security Policy), authorizing and monitoring access to this information, and agreeing on appropriate measures to prevent unauthorized access.

- Information Guardians are responsible for working with the CSO to investigate and manage suspected breaches (incidents). These suspected breaches shall be reported by the CSO to the Chief Executive Officer ("CEO"). In absence of the CEO, the CSO will report any suspected breaches to the President.
- The CSO is responsible for preparing written recommendations to the CEO related to any actions that need to be taken to mitigate both IT security risks and physical security risks.
- Based on consultation with the CEO (and President when the CEO is unavailable) the CSO will take appropriate action related to breaches and potential breaches of IT systems and network security.
- The CSO is responsible for reporting, investigating, and taking appropriate action to address breaches of physical security and suspected attempts to gain unauthorized access to secure areas and for escalating incidents to the CEO who has ultimate responsibility for information security.

Investigation and Potential Notifications Related to a Breach

When a breach or potential loss of data is reported, the Chief Executive Officer will be responsible for quickly and responsibly investigating the alleged incident. The investigation will be managed by the Chief Executive Officer in conjunction with the Chief Security Officer and any other relevant individuals from within the organization or outside the organization. If it is determined that there has been a breach and relevant information has been accessed or, information can be potentially acquired through the loss of data (equipment, etc.), the effected individuals or entities will be promptly notified. If required or deemed necessary, relevant government entities will be notified. If the data is HIPAA data, TMA will follow the procedures set forth by the U.S. Department of Health & Human Services. These procedures are provided on the "hhs.gov" website under Health Information Privacy – Breach Notifications.

Responsibility for Creating a Culture of Information Security

The CSO has the ultimate responsibility for security management and for providing proactive leadership to instill a culture of information security within the Company. The CSO will do this through providing clear direction, demonstrating commitment to information security, providing explicit assignments to meet the information security levels desired by the Company, and proper acknowledgement of information security policies.

III. Procedure

There is no content for this section.

IV. Who is affected by this Policy

All Company employees and consultants are affected by this policy.

V. Definitions

There is no content for this section.

VI. Related Policies

- **Information Security Policy Framework**
- **Information Security Policy**
- **Information Security Plan**
- **Information Security Password Policy**
- **Information Technology Policy**
- **Network Administrative Security Policy**
- **Data Encryption Policy**
- **Monitoring and Logging Policy**
- **Business Continuity Policy**
- **Disaster Recovery Policy and Plan**

VII. Update Log

June 1, 2015: Policy issued.