Infrastructure Security Policy Framework

Policy Title	**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	July 1, 2021

I. Policy Statement

TMA Systems possesses information corporately, for their clients, and for their business associates that is sensitive and valuable. If accessed by unauthorized individuals, tampered with, or made unavailable, it could cause irreparable harm for this group. Therefore, TMA has produced a series of Information Security and Information Technology policy statements (the "Framework") to minimize or alleviate this risk. As a group of documents, this data will assist the organization in organizing, measuring, and managing information risk.

The Framework establishes high-level information security requirements. The Framework also provides the mandate for the organization to establish TMA's support for promoting information security in all of its practices.

These policies are living documents that will change for a variety of reasons including, but not limited to: changes in technology, changes in methods of access, changes in information sensitivity levels and changes in the Company business.

II. Policy

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

Information Security Policy

The Information Security Policy is the standard policy related to TMA's of protection of information. It focuses on the different types of information, sensitivity levels, obligations to 3rd parties, basic requirements for computers, and federal and state laws.

Information Security Plan

The TMA Systems' Information Security Plan ("ISP") establishes and states the plans and protocols for achieving and maintaining internal control over information systems as well as compliance with the standards set by the company. The ISP is designed to protect information and critical resources from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return-on-investment for business opportunities.

Information Security Password Policy

TMA Systems Information Security Password Policy describes the Company's requirements for acceptable password selection and maintenance to maximize security of passwords and minimize the passwords misuse or theft.

Information Security Incident Management

The Information Security Incident Management Policy deals with security incidents: what they are, how to deal with them, where the policy applies and lines of responsibility. Most importantly, 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.

Information Technology Policy

The Information Technology Policy deals with acceptable use of TMA Systems IT and digital resources. It defines acceptable uses for provisioning information technology resources at TMA Systems and the associated responsibility of authorized users when accessing these information technology resources. These resources include, but are not limited to, TMA Systems' network, computer systems and software, access to the Internet, electronic mail, telephony and related services.

Network Administrative Security Policy

TMA Systems must maintain secure networks to protect sensitive and valuable information both corporately, for their clients, and for their business associates. Network Administration defines the roles, responsibilities and privileges related to “proper privileges” and policies related to “patch management”.

Encryption Key Policy

The Encryption Key Policy sets forth the basic information required to effectively and efficiently plan, prepare and deploy encryption solutions in order to secure restricted information (Sensitive Data). The primary goal of the policy is to provide encryption solutions that preserve the confidentiality and integrity of, and control accessibility to, data classified as "Legally or Contractually Restricted" where this data is processed, stored or transmitted.

Monitoring and Logging Policy

Monitoring and logging of Company systems will be carried out in order to protect the safety, confidentiality, integrity and availability of information within the organization. Monitoring provides information to manage network traffic resources, user and system activity, faults and external or internal threats. Logging records these events in order to report activity and provide an audit trail.

Business Continuity Policy

TMA Systems, like any other firm, is exposed to potential risks that could disrupt or destroy critical business functions and/or the production and delivery of services. Our strategy for continuing business in the event of an incident is to ensure the safety and security of all employees; and to continue critical business functions, production and delivery of services from predefined alternative sites. The purpose of the BC/DR policy is to ensure that all business activities can be kept at normal or near-normal performance following an incident that has the potential to disrupt or destroy the Company.

Disaster Recovery Policy and Plan

Disaster recovery refers to the criteria and procedures used to guide management and technical staff in the recovery of computing and network facilities operated by the organization in the event that a disaster destroys all or part of the facilities or, the recovery of data related to a breach or other Information Security Incident. This policy should be read in conjunction with the “Information Security Incident Management Policy”.

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**
- **Information Security Plan**
- **Information Security Password Policy**
- **Information Security Incident Management**
- **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.