Information Security Plan

Policy Title	**Information Security Plan** **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	July 1, 2021

I. Policy Statement

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.

The purpose of this plan is to ensure the confidentiality, integrity, and availability of data, define, develop, and document the information policies and procedures that support the Company's goals and objectives, and to allow the Company to satisfy its legal and ethical responsibilities with regard to its IT resources.

Information security policies and procedures represent the foundation for the Company's ISP. Information security policies serve as overarching guidelines for the use, management, and implementation of information security throughout the Company.

Internal controls provide a system of checks and balances intended to identify irregularities, prevent waste, fraud and abuse from occurring, and assist in resolving discrepancies that are accidentally introduced in the operations of the business. When consistently applied throughout the organization, these policies and procedures assure that information technology resources are protected from a range of threats in order to ensure business continuity and maximize the return on investments related to our business interests.

This plan reflects the Company's commitment to stewardship of sensitive information, in acknowledgement of the many threats to information security and the importance of protecting the privacy of client's information, safeguarding vital business information, and fulfilling legal obligations. This plan will be reviewed and updated at least once a year or when the environment changes.

II. Policy

- **Information Security Program**
- **Risk Assessment**
- **Virus Protection**
- **Backup and Recovery**
- **Backup and Recovery Standard**

Information Security Program

Through this document and associated policies, TMA Systems has established, documented, and implemented an Information Security Program. The system is designed to result in improving the effectiveness of IT operations and ability to satisfy regulatory requirements. This program has been implemented to ensure the confidentiality and integrity of information (both Company and Client) while maintaining appropriate levels of accessibility.

In order to ensure the security and confidentiality of sensitive information and to protect against any anticipated threats or hazards to the security or integrity of data, the Company has put in place all reasonable technological means, (i.e., security software, hardware) to keep information and facilities secure. The Company has defined its own security controls, which are to be equal to or greater than security requirements and controls prescribed by law or client requirements.

Risk Assessment

A risk assessment is a process which determines what information resources exist that require protection, and to understand and document potential risks from IT security failures that may cause loss of information confidentiality, integrity, or availability. The purpose of a risk assessment is to help management create appropriate strategies and controls for stewardship of information assets. Because economics, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

Objectives must be established before management can identify and take necessary steps to manage risks. Operations objectives relate to effectiveness and efficiency of the operations, including performance and financial goals and safeguarding resources against loss. Compliance objectives pertain to laws and regulations which establish minimum standards of behavior.

The Company will conduct an annual risk assessment and/or business impact analysis in order to:

- Inventory and determine the nature of Company information resources
- Understand and document the risks in the event of failures that may cause loss of confidentiality, integrity, or availability of information resources
- Identify the level of security necessary for the protection of the resources.

Virus Protection

Viruses are a threat to the Company as infected computers may transmit confidential information to unauthorized third parties, provide a platform for unauthorized access or use of the internal network, contaminate or infect other network connected devices, or interfere with Company information technology resources. Antivirus software is provided to the organization to protect against the damage caused by virus attacks. Network administrators are responsible for creating procedures to ensure anti-virus software has the latest updates and virus signatures installed and also to verify that computers are virus-free.

TMA Systems reserves the right to review any device attached to the network (public or non-public) for adequate virus protection. The Company reserves the right to deny access to the network to any device found to be inadequately protected. Additionally, the Company reserves the right to disable network access to any device that is insufficiently protected, or currently infected with a virus. Network access may be restored when the device has been cleaned and current antivirus software and applicable operating system and application patches have been installed.

Backup and Recovery

All electronic information is to be copied onto secure storage media on a regular basis (i.e., backed up), for the purpose of disaster recovery and business resumption based on the Backup and Recovery Standard outlined below. The Backup and Recovery Standard outlines the minimum requirements for the creation and retention of backups. Special backup needs which exceed these minimum requirements, may be accommodated on an individual basis.

All backups must conform to the following best practice procedures:

- All data and utility files must be adequately and systematically backed up.

  (Ensure this includes all patches, fixes and updates)
- Records of what is backed up and to where must be maintained
- Records of software licensing should be backed up

Backup and Recovery Standard

All electronic information considered of value should be copied onto secure storage media on a regular basis (i.e., backed up), for disaster recovery and business resumption. This policy outlines the minimum requirements for the creation and retention of backups. Special backup needs, identified through technical risk analysis that exceeds these requirements, should be accommodated on an individual basis.

Scope

Data custodians are responsible for providing adequate backups to ensure the recovery of data and systems in the event of failure. Backup provisions allow business processes to be resumed in a reasonable amount of time with minimal loss of data. Since hardware and software failures can take many forms, and may occur over time, multiple generations of proper data backups need to be maintained.

Standard

Backup and Recovery processes commensurate with legal and business requirements must be developed, maintained and regularly tested, to ensure continued business operation and access to data and information within the required timeframe, should a risk event occur.

Backup Requirements will be determined by a business risk assessment completed by the owner, and is dependent on:

- Importance of the data and information to the function of the Company, clients, partners, or their respective employees.
- Acceptable transaction loss (business areas must determine what level of potential transaction loss would not be acceptable or would be too difficult to recover. This can be determined in terms of a timeframe, the number of transactions, or the amount of effort and period of time required re-entering data.
- The maximum acceptable outage of the system while performing backups
- The maximum acceptable outage of system while recovering data

In addition to regular backup processes, backups will be performed before and after major technical or business related changes to a system or application.

An audit trail of all backup activities must be maintained.

Documentation

For all information assets, documented procedures must exist for the backup and recovery processes and these documents must be readily accessible. Backup and recovery operations and the specified period of maximum acceptable outage must be documented for all systems.

At a minimum documentation must contain:

- A description of the system to be backed up
- The individual or group responsible for ensuring that the backup and recovery occurs
- Backup and recovery requirements
- Backup media storage locations, including off-site storage
- Required backup frequency e.g. daily, weekly
- Backup cycles required
- Backup retention period (as prescribed by the Company Data Retention Policy)
- Testing process
- Recovery schedule and plan
- Locations of relevant software and licenses

Backup Media

Backups must be regularly tested as determined by a risk assessment or at a minimum on an annual basis to ensure data can be restored in case of a catastrophic event.

Protection mechanisms and access controls for backup media must be commensurate with the security requirements and criticality of the information stored in the backup.

Backup media must be stored and transported in an appropriate, safe and secure manner and access to backup media must be restricted to only authorized personnel.

Off-site Storage

Based on backup requirements and backup cycles, at least one instance of a backup within a cycle must be stored off-site (physically separate from the data or system being backed up) or geographically separate, as determined by a risk assessment.

Backup media stored off-site must be stored in a secure location with environmental controls (if available) and appropriate access controls commensurate with the security requirements and criticality of the information stored in the backup.

Back-up media will be stored off-site on a basis that is determined by the risk assessment.

Backup Media Disposal

Obsolete backup media must be disposed of in a safe and secure manner. Backup media to be disposed of must be rendered unreadable through an appropriate means and an audit trail of disposal of backup media must be maintained.

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 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.