Information Security Policy

Policy Title	**Information Security 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

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

TMA Systems possesses information corporately, for their clients, and for their business associates that is sensitive and valuable, e.g., personally identifiable information, financial data, research data, various client data, and other information considered sensitive. Some information is protected by federal and state laws or contractual obligations that prohibit its unauthorized use or disclosure. The exposure of sensitive information to unauthorized individuals could cause irreparable harm to the Company, clients, partners, or their respective employees, it could also be subject to fines or other government sanctions. Additionally, if the information were tampered with or made unavailable, it could impair these organization's ability to do business. The Company therefore requires all employees to diligently protect information as appropriate for its sensitivity level.

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

II. Policy

- **Summary of Responsibilities**
- **Information Collection and Guardians**
- **Information Sensitivity Levels**
- **Personally Identifiable Information (PII)**
- **Directory Information**
- **Requirements for Computers Used to Conduct Company Business**
- **Managing Confidential and/or Highly Confidential Information**
- **Contractual Obligations**
- **Federal and State Laws Mandating Information Protection**

Summary of Responsibilities

All employees and contractors

1. You may only access information needed to perform your legitimate duties as a Company employee and only when authorized by the appropriate Information Guardian or designee. (Corporate Information Guardians and contacts)
2. You are expected to ascertain and understand the sensitivity level of information to which you have access through training, other resources or by consultation with your manager or the Information Guardian.
3. You may not in any way divulge, copy, release, sell, loan, alter or destroy any information except as authorized by the Information Guardian within the scope of your professional activities.
4. You must understand and comply with the Company's requirements related to personally identifiable information (PII).
5. You must adhere to the Company's requirements for protecting any computer used to conduct corporate business for any computers used to transact corporate business regardless of the sensitivity level of the information held on that system.
6. You must protect the confidentiality, integrity, and availability of the corporate information as appropriate for the information's sensitivity level wherever the information is located, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.
7. Information deemed Confidential or Highly Confidential under this policy must be handled in accordance with the Company's requirements for protecting Confidential and Highly Confidential information.
8. You must safeguard any physical key, ID card or computer/network account that allows you to access corporate information. This includes creating difficult-to-guess computer passwords.
9. You must destroy or render unusable any confidential or highly confidential information contained in any physical document (e.g., memos, reports, microfilm, microfiche) or any electronic, magnetic, or optical storage medium (e.g., USB key, CD, hard disk, magnetic tape, diskette) before it is discarded.
10. You must report any activities that you suspect may compromise sensitive information to your supervisor or to the Company’s Chief Security Officer.
11. Your obligation to protect sensitive information continues after you leave the Company.
12. While many federal and state laws create exceptions allowing for the disclosure of confidential information to comply with investigative subpoenas, court orders and other compulsory requests from law enforcement agencies, anyone who receives such compulsory requests should contact the Chief Executive Officer or the Company’s General Counsel before taking any action.
13. If you are performing work in an office that handles information subject to specific security regulations, you will be required to acknowledge that you have read, understand and agree to comply with the terms of this policy annually.

Managers and supervisors

In addition to complying with the requirements listed above for all employees and contractors, managers and supervisors must:

1. Ensure that departmental procedures support the objectives of confidentiality, integrity and availability defined by the Information Guardian and designees, and that those procedures are followed.
2. Ensure that restrictions are effectively communicated to those who use, administer, capture, store, process or transfer the information in any form, physical or electronic.
3. Ensure that each staff member understands his or her information security-related responsibilities.

Technology managers

In addition to complying with the policy requirements defined for all employees and contractors, and managers and supervisors, those who manage computing and network environments that capture, store, process and/or transmit corporate information, are responsible for ensuring that the requirements for confidentiality, integrity, and availability as defined by the appropriate Information Guardian are being satisfied within their environments. This includes:

1. Understanding the sensitivity level of the information that will be captured by, stored within, processed by, and/or transmitted through their technologies.
2. Developing, implementing, operating, and maintaining a secure technology environment that includes:
    - A cohesive architectural policy,
    - Product implementation and configuration standards,
    - Procedures and guidelines for administering network and system accounts and access privileges in a manner that satisfies the security requirements defined by the Information Guardians, and
    - An effective strategy for protecting information against generic threats posed by computer hackers that adheres to industry-accepted "best practices" for the technology.
3. Ensuring that staff members understand the sensitivity levels of the data being handled and the measures used to secure it.

Information Guardians

In addition to complying with the requirements listed above, Information Guardians are responsible for:

1. Working with the Chief Security Officer and the General Counsel to understand the restrictions on the access and use of information as defined by federal and state laws and contractual obligations.
2. Segregating the information for which they are responsible into logical groupings, called information collections,
3. Defining the confidentiality, integrity and availability requirements (sensitivity level) for each of their information collections.

4. Conveying in writing the sensitivity level of each information collection for which they are responsible to the managers of departments that will have access to the collection,
5. Working with department managers to determine what users, groups, roles or job functions will be authorized to access the information collection and in what manner (e.g., who can view the information, who can update the information).

Information Collection and Guardians

Corporate-held information must be protected against unauthorized exposure, tampering, loss and destruction, wherever it is found, in a manner that is consistent with applicable federal and state laws, the Company's contractual obligations, and with the information's significance to the Corporation as well as any individual whose information is collected. Achieving this objective requires that:

- The information's sensitivity level must be defined to convey what level of protection is expected to all employees/agents who are authorized to access the information.
- The individuals who should have access to sensitive information must be identified, either by role or by name.

For purposes of managing information, the Company's various types of information must be segregated into logical collections (e.g., medical records, employee benefit data, payroll data, client data, financial records, and other data deemed sensitive). Each collection must be "managed" by an individual known as an "Information Guardian," who must:

- Define the collection's sensitivity level consistent with this policy,
- Convey the collection's requirements to the managers of departments that will have access to the collection,
- Work with office heads and chairs to determine what users, groups, roles or job functions are authorized to access the information in the collection and in what manner (e.g., who can view the information, who can update the information).

The guardian of an information collection is typically the head of the department on whose behalf the information is collected or that is most closely associated with such information. Each Information Guardian may designate one or more individuals on their staff to perform the above duties. However, the Information Guardian retains ultimate responsibility for their actions.

TMA Systems Information Guardians:

Overall Corporate:	Chief Executive Officer
Overall Corporate:	President (Designated)
Sales & Marketing:	Director of Sales & Marketing
Operations:	Director of Operations
Engineering:	Director of Advanced Technology
Administrative:	Director of Administration

Information Sensitivity Levels

Information Guardians are responsible for assessing the security requirements for each of their assigned information collections across three areas of concern: confidentiality, integrity and availability.

To facilitate the assessment process and ensure that these requirements are expressed in a consistent manner across the Company, Information Guardians should categorize their information collections using the levels described in this section.

The **confidentiality** requirement for an information collection will be expressed in the following terms:

- "**Public**" information can be freely shared with individuals within or outside the Company without any further authorization by the appropriate Information Guardian/designee.
- "**Internal**" information can be freely shared with TMA Company Employees. Sharing such information with individuals outside of the Company requires authorization by the appropriate Information Guardian/designee.
- "**Departmental**" information can be freely shared with members of the owning department. Sharing such information with individuals outside of the owning department requires authorization by the appropriate Information Guardian/designee.
- "**Confidential**" information can only be shared on a "need to know" basis with individuals who have been authorized by the appropriate Information Guardian/designee, either by job function or by name.
- "**Highly confidential**" information can only be shared on a "need to know" basis with a limited number of individuals who have been identified by the appropriate Information Guardian/designee.

The **integrity/availability** requirement for an information collection will be expressed as follows:

- Information is "**non-critical**" if its unauthorized modification, loss or destruction would cause little more than temporary inconvenience to the user community and support staff and incur limited recovery costs. Reasonable measures to protect information deemed "non-critical" include storing physical information in locked cabinets and/or office space, using standard access control mechanisms that prevent unauthorized individuals from updating computer-based information, and making regular backup copies.
- Information is "**Critical**" if its unauthorized modification, loss, or destruction through malicious activity, accident or irresponsible management could potentially cause the Company to:
    - Suffer significant financial loss or damage to its reputation,
    - Be out of compliance with legal/regulatory or contractual requirements,
    - Adversely impact its clients or the Company.
- Additional safeguards for "**Critical**" information:
    - "Critical" information must be verified either visually or against other sources on a regular basis, and
    - A business continuity plan to recover "critical" information that has been lost or damaged must be developed, documented, deployed and tested annually.

Personally Identifiable Information (PII)

Personally Identifiable Information (or "PII," as used in this Policy) is information that can be used (either alone or in combination with other information) to identify, contact or locate a unique person. Examples include (but are not limited to): name, social security number, address, birth date, telephone number, account numbers, etc.

All Personally Identifiable Information in the possession of the Company is considered Confidential unless:

1. The information is designated as "Directory Information" by the appropriate Information Guardian; or
2. The Information Guardian has otherwise authorized its disclosure.

The Company requires that the following pieces of PII may not be collected, stored or used except in situations where there is legitimate business need and **no reasonable alternative**:

- Social Security Number,
- Date of birth,
- Place of birth,
- Mother's maiden name,
- Credit card numbers,
- Bank account numbers,
- Income tax records, and
- Driver's license numbers.

Managers must ensure that their employees understand the need to safeguard this information, and that adequate procedures are in place to minimize this risk. Access to such information may only be granted to authorized individuals on a need-to-know basis.

Directory Information

All Personally Identifiable Information in the possession of the Company is considered Confidential unless designated as "Directory Information" by the appropriate Information Guardian or otherwise authorized to be disclosed.

Directory information for current and former employees

The Company generally prohibits the disclosure of information regarding current and former employees that was created or collected during their employment. However, the Company allows for the disclosure of this type of "directory information" unless an employee has expressly objected to such disclosure.

The relevant Information Guardians define the following to be “Directory Information” that may be shared:

- Name
- Address (the Guardians require that it be treated as “Internal” and not disclosed absent a compelling reason)
- Title and/or job function
- Telephone number
- E-mail address
- Photo
- Dates of their affiliation with the Company

For information about providing references for former employees, please contact Human Resources.

Requirements for Computers Used to Conduct Company Business

To adequately protect Company information systems from compromises, all computers used to conduct Company business must be configured using security industry-sanctioned best practices that include but are not limited to the following:

- Configure and use computers in a manner that is compliant with the Company's core technology policy which is defined in the Information Technology Policy.
- Require all computer accounts to have strong passwords as defined by the Information Security Password Policy.
- Define accounts intended for day-to-day computer use as "general user accounts". Accounts that have administrative privileges must only be used for system setup and maintenance.
- Computers should be configured to "time out" after no more than 30 minutes of inactivity.
- Users should lock or log off their computers before leaving them unattended.
- Ensure that system and application security updates are applied as soon after being released by the vendor as possible.
- Ensure that anti-virus software is installed and is actively protecting the system.
- Limit the services running on Company computers to those needed by the computer user to perform their assigned tasks.
- Ensure that any system is configured to keep a record of:
    - Who attempted to log into the system (successfully and unsuccessfully) and at what time.
    - When they logged out,
    - Administrative activity performed,
    - Unsuccessful attempts to access confidential and highly confidential files.

Managing Confidential Information and/or Highly Confidential Information

No one may access information that has been classified as Confidential and/or Highly Confidential without authorization by the appropriate Information Guardian. For information classified as Confidential, such authorization may be granted to individuals by name or to all individuals serving in a specific job function. For information classified as Highly Confidential, access must be authorized for everyone by name.

For information classified as Confidential or Highly Confidential, the following procedural and system-level controls must be in place:

- Access to Confidential or Highly Confidential Information collection may only be granted after receiving permission by the appropriate Information Guardian/designee authorizing such access. The authorization by the appropriate Information Guardian/designee must be documented either by physical or electronic form.
- Departmental procedures must be in place to ensure that all individuals who have access to Confidential or Highly Confidential information are aware of the sensitivity of the information to which they have access, understand their responsibilities to protect that information appropriately, and acknowledge their understanding and intent to comply with this policy.
- Tangible records (paper documents, microfilm, etc.) containing Confidential or Highly Confidential information must be:
    - Stored in a locked cabinet or drawer when not in use with access limited to authorized individuals, and
    - Physically shredded/destroyed when no longer needed.
- In addition to the requirements for all computers used to conduct Company business, computers that accept, capture, store, transmit or process information classified as Confidential or Highly Confidential must comply with the following requirements:
    - Any piece of Confidential or Highly Confidential Information should be transmitted via the encrypted tmasystems.net customer portal or the secure VPN tunnel which has been approved by the Company CSO.
    - Laptops, other mobile and external storage devices holding information designated as confidential or highly confidential must:
        - Have the information on their drives encrypted using an encryption product and methodology approved by the Company CSO, except when domestic or international laws prohibit the use of encryption software.
        - Where technically feasible, only be usable by a limited number of specific users and system administrators explicitly authorized by the department that owns the laptop. Note - While traveling to most countries with our standard encryption software on your laptop or mobile device requires no action on your part, there are a few nations to which transporting encryption software without a proper license could violate domestic or international law. **When traveling to any country in this category, both the encryption software and all Confidential and Highly Confidential information must be removed from your system prior to your departure.** To determine whether any country on your itinerary falls into this category, please discuss with the Company CSO.

- Computer servers must:
    - Be secured by a hardware firewall, approved by the CSO, which only permits connections with authorized systems using approved protocols.

Contractual Obligations

Agreements protecting another entity's information

Company employees are responsible for complying with the terms of contracts or agreements that may limit the ability to disclose confidential information belonging to (or collected on behalf of) another organization. Employees are expected to educate themselves about the limitations imposed on the information to which they have access, including contractual obligations. Some examples of these arrangements are:

- Non-disclosure agreements when research information developed by another organization is shared with the Company
- Non-disclosure agreements where the external entity shares pre-release product information,
- End user licensing agreements associated with commercial software, shareware, freeware and other software,
- Contractual obligations with external entities requiring compliance with their security standards.

Agreements protecting Company information

When negotiating contracts with external entities, Company employees should consider whether there are any alternatives to giving members of the other organization access to Company databases or other filing systems containing sensitive information.

If such access is necessary, agreements that provide the outside entity with access must ensure that the employees/agents of the entity are required to maintain confidentiality consistent with the Company's obligations and interests. In addition, outside employees/agents should be contractually obligated to implement data protection and security measures that are commensurate with the Company's practices.

Federal and State Laws Mandating Information Protection

As summarized below, several federal and state laws may also apply to information collected and maintained by the Company and its employees. Please direct questions regarding the applicability of these laws and other potential legal issues to the Company's General Counsel.

Key Statutes

Health Insurance Portability and Accountability Act (HIPAA)

Enacted in 1996, HIPAA imposes obligations on health plans, health care clearinghouses, and health care providers to protect health information when electronically transmitted. As a provider of self-insured group health plans, the Company is subject to certain HIPAA requirements. Therefore, certain offices must take steps to appropriately manage contracts with business associates, complete training on applicable privacy policies and procedures and/or complete a confidentiality acknowledgement. HIPAA may also apply to certain research activities such as the collection and use of personally identifying health information from patient populations in clinical settings. Further information regarding compliance with HIPAA is available through the Company's General Counsel.

Other Statutes and Restrictions

Computer Fraud and Abuse Act (CFAA)

Enacted in 1984 (and revised in 1994), the CFAA criminalizes unauthorized access to a "protected computer" with the intent to defraud, obtain any information of value or cause damage to the computer. Under the CFAA, a "protected computer" is defined as a computer that is used in interstate or foreign commerce or communication or that is used by or for a financial institution or the government of the United States. For example, the act of "hacking" into a secure web site from an out-of-state computer may violate the CFAA.

Electronic Communications Privacy Act (ECPA)

Enacted in 1986, the ECPA broadly prohibits (and makes criminal) the unauthorized use or interception of the contents or substance of wire, oral or electronic communications. In addition, the ECPA prohibits unauthorized access to or disclosure of electronically stored communications or information. Such prohibitions may apply to Company employees who willfully exceed the scope of their duties or authorizations by accessing certain databases housed within the Company system. The ECPA does not, however, prohibit the Company from monitoring network usage levels and patterns to ensure the proper functioning of its information systems.

State Laws

In addition to the federal laws summarized above, there may be state laws that apply to the handling of confidential information. For example, state laws may govern the collection or use of information regarding children, consumers, and other groups. Before establishing new practices regarding the handling of confidential information, Company employees are encouraged to consult the Company's General Counsel to determine whether specific laws apply.

Subpoenas and Other Compulsory Requests

Many of the federal and state laws described above create exceptions allowing for the disclosure of confidential information to comply with investigative subpoenas, court orders and other compulsory requests from law enforcement agencies. Employees who receive such compulsory requests should contact the Company's General Counsel before taking any action.

Access to Information under Vendor Agreements

When negotiating contracts with third party vendors, Company's employees should consider whether such vendors require access to Company databases or to other filing systems containing confidential information. Agreements providing third party vendors with access to such information must ensure that the vendor is subject to obligations of confidentiality that will enable the Company to comply with its own obligations under the applicable privacy laws. In addition, such vendors should be contractually obligated to implement data protection and security measures that are commensurate with the Company's practices. By the same token, Company employees must be careful not to disclose confidential information entrusted to their care by an outside party, especially when such information is governed by the terms of a confidentiality agreement or clause with that party.

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 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.
