# Data Encryption Policy

| | |
|---|---|
| **Policy Title** | **Data Encryption Policy**<br>**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

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. This policy provides the basic information required to effectively and efficiently plan, prepare and deploy encryption solutions in order to secure "Restricted Information" (Sensitive Data). These guidelines apply to all devices, physical or virtual where data is classified as "Restricted Information". This data could be Confidential, Highly Confidential or at times PII (Personal Identifiable Information).

The Company's primary goal 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.

Individuals should understand that data encryption is not a substitute for other information protection controls, such as access control, authentication, or authorization; that data encryption should be used in conjunction with those other controls; and that data encryption implementations should be proportional to the protection needs of the data.

## II. Policy

- **Encryption Applicability**
- **Encryption Services**
- **Encryption Key Management**
- **Responsibilities**
- **Legal and Contractual Requirements**

## Encryption Applicability

1. Transmission: In order to protect the confidentiality and integrity of sensitive data; any data classified as Restricted Information, and having a required need for confidentiality and/or integrity, shall be transmitted via encrypted communication to ensure that it does not traverse the network in clear text.
2. Storage: In order to protect the confidentiality and integrity of data classified as Restricted Information: this data will have the requirement of being stored in encrypted systems and/or databases and/or portable media. Data not classified as Restricted Information will not require such encrypted storage.
3. A combination of business practices and technology can act as mitigating factors and could significantly reduce the risk of unauthorized data exposure, thereby offsetting the specific need to implement data encryption. These would need to be reviewed by the Chief Security Officer for recommendation to the Chief Executive Officer for his approval.

## Encryption Services

1. The symmetric algorithms shall be used for encrypting Restricted Information.
2. The asymmetric algorithms shall be used for public key encryption for Restricted Information.
3. Digital signatures shall be used to associate a user or entity with a respective public key.
4. Digital certificates shall apply recognized standards and shall at least:
    - Identify the issuing certificate authority; the certificate authority shall be one authorized by Chief Security Officer or strictly designated for internal usage
    - Identify its subscriber
    - Provide the subscriber's public key
    - Identify its operational period
    - Be digitally signed by the issuing certificate authority

## Encryption Key Management

1. Encryption Keys used to protect Restricted Information shall also be considered Restricted Information.
2. Proper control of Encryption Keys is critical to prevent unauthorized disclosure of Restricted Information or irretrievable loss of important data. The control and management of the Encryption Keys shall be overseen by the Chief Security Officer.
3. All symmetric encryption keys used on systems associated with Restricted Information shall be randomly generated according to industry standards.
4. Where symmetric encryption is used to protect Restricted Information:
    - Master keys shall be changed at least once per year.
    - Primary encrypting keys shall be changed at a minimum of twice per year.
    - Data encrypting keys shall be changed once per session or every 24 hours.
5. When asymmetric encryption is used, the operational period of asymmetric keys associated with a public key certificate are defined by the encryption key management plan of the issuing certificate authority.
6. Encryption keys are confidential information, and access shall be strictly limited to those who have a need-to-know.
7. Encryption keys that are compromised (e.g., lost or stolen) shall be reported immediately to the Chief Security Officer, the Chief Executive Officer, and the information owner of the data being protected. The key shall be revoked or destroyed and a new key generated. Key re-assignments shall require re-encryption of the data.

---

## Responsibilities

Chief Security Officer: The Chief Security Officer will be responsible for maintaining and overseeing the Data Encryption Policy which is used to protect Restricted Information.

User Responsibilities: All users shall be responsible for adhering to the Company's Data Encryption Guidelines and related policies. Users must manage the storage and transmission of data in a manner that safeguards and protects the confidentiality, integrity, and availability of such data.

Questions about classification of data or guidelines should be directed to the Chief Security Officer.

### Legal or Contractual Requirements

There may be a number of federal and state laws, as well as contractual requirements, that 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.

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

# VII. Update Log

June 1, 2015: Policy issued.