Business Continuity Policy

Policy Title	**Business Continuity 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	January 1, 2018
Last Update	April 1, 2022

I. Policy Statement

TMA Systems is committed to providing the best possible experience to its clients and the best possible relationships with employees and suppliers. To ensure the consistent availability and delivery of its services, TMA Systems has developed the following business continuity and disaster recovery (BC/DR) policy in support of a comprehensive program for BC, DR and overall business survivability.

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.

II. Policy

- **Policy Leadership**
- **Verification of Policy Compliance**
- **Penalties for Non-Compliance**

Policy Leadership TMA Systems LLC

Stuart Zimmerman, Director of Engineering and Technical Operations, is designated as the Corporate Management Liaison responsible for the BC/DR program. Resolution of issues in the development of, or support of, all BC/DR plans and associated activities should first be coordinated with the BC/DR Team and appropriate internal or external organizations before submitting to the corporate management liaison. The issue resolution process is defined in the following section.

Contact Information: (Cell) 918-237-9594
BC/DR Team:

Dustin Taylor, President	918-606-2494
John Swofford, Director of Sales	918-284-9109
Tabor Ellison, Dir of Development – RiskPartner	918-808-9515
Patrick Smith, Director of Advanced Technology	918-630-0401
Stuart Zimmerman, Chief Operating Officer	918-237-9594
Adam Deatherage, Dir of Client Services	918-346-3915

Verification of Policy Compliance

BC/DR compliance verification is managed by the BC/DR Team with support from other relevant internal departments. The plan must define appropriate procedures, staffing, tools and workplace planning activities necessary to meet compliance requirements.

BC/DR Compliance Verification is required annually and is facilitated by the BC/DR Team.

Penalties for Non-Compliance

In situations where a Company department does not comply with the BC/DR policy, the BC/DR Team will prepare a brief statement explaining the non-compliance and present it to the BC/DR corporate management liaison for resolution. Failure to comply with BC/DR policies within the allotted time for resolution may result in verbal reprimands, notes in personnel files, termination and other remedies as deemed appropriate.

III. Procedure

All individuals noted above (Corporate Management Liaison/ BC/DR Team) will be on a “Group Text” to provide notification of meeting at designated location. This location will be the Downtown

Tulsa Hyatt hotel unless otherwise agreed to.

Facilities: The company has planned with the Downtown Hyatt to provide adequate space for 50% of the staff to work. (See confidential facilities information Addendum A)

Equipment: Backup equipment is stored at the Hyatt and applications are updated quarterly. (See confidential equipment information Addendum B)

Data: Relevant data for operations is backed up at our offsite data facility on a weekly basis. (See confidential data information Addendum C)

Annual Test: An annual test is conducted every April prior to the annual TMA User Conference.

Communications: Determining the communication strategy (messages and notification lists) or changes to the strategy will start with the CEO and work down the BC/DR Team list. Communications in order of priority:

- Employees – This is the first team to communicate with. The first line of communications will be via cell phone (text/voice). The next lines of communications will be landline phones, email and the final line of communications will be direct contact at their residences. (Human Resources will be responsible for maintain up-to-date employee lists)
- Clients – The CEO and the BC/DR Team will determine which clients will be affected. Communications will begin with e-mail notifications and move to phone communications. (Client Lists will be maintained by the Client Relations Management Department)
- Vendors - The CEO and the BC/DR Team will determine which vendors will be affected. Communications will begin with e-mail notifications and move to phone communications. (Vendor Lists will be maintained by the Administration Department)

IV. Who is affected by this Policy

All Company employees, consultants, customers and suppliers 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**
- **Data Encryption Policy**
- **Monitoring and Logging Policy**
- **Disaster Recovery Policy and Plan**

VII. Update Log

January 1, 2018: Policy issued.
