Disaster Recovery Policy and Plan

Policy Title	**Disaster Recovery Policy and 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	April 1, 2022

I. Policy Statement

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".

II. Policy & Plan

- **Purpose of Policy**
- **Disaster Planning – Disaster Risk and Prevention**
- **Disaster Planning – Preparation**
- **Disaster Plan – Activation**
- **Equipment, Assessment, Protection and Salvage**
- **Platform Recovery Procedures**
- **Basic Information about Systems**
- **Maintaining the Plan**
- **Who the Policy Applies to**
- **Where the Policy Applies**

Purpose of Policy

The mission critical dependence upon the use of computers in the day-to-day business activities of our organization and our client's business operations has become standard. Building a strong Disaster Recovery Plan supports the prompt and consistent recovery for both our operations and the recovery of our data. Most importantly, recovery and bringing our client's back on-line is paramount in minimizing any harm to their organizations.

Disaster Planning – Risk and Prevention

As important as having a disaster recovery plan is, taking measures to prevent a disaster or to mitigate its effects beforehand is even more important. This portion of the plan reviews the various threats that can lead to a disaster, where our vulnerabilities are, and steps we should take to minimize our risk. The threats covered here are both natural and human-created.

- Fire
- Flood
- Tornados and High Winds
- Earthquake
- Computer Crime
- Terrorist Actions and Sabotage

The overall risk for our organization is low. We have both solid facilities with low risk for fire, flood tornados, high winds and earthquakes, security personnel on the grounds of our facilities and a security system limiting access to authorized personnel based on their access rights.

The above, are our primary risks. Some are greater than other. A short synopsis of these risks are as follows:

Fire: Low Risk - We have some risk because we are in a shared facility. The facility is a steel and stone construction and is annually inspected by the development company's Risk Assessment Group and insurance carrier – mitigation measures are carried out. Highest risk is smoke damage.

Flood: Low risk and on third floor of facility in an area that is not a flood plain.

Tornados and High Winds: Medium risk – Area has had tornados. Structure is steel and stone however, large windows carries risk. This area is lounge and eating facility. Internal server area is well protected and work areas have modest exposure.

Earthquake: Low risk. Area has not been subject to earthquakes.

Computer crime: Medium risk "Information Security Policy Framework" reduces this exposure.

Terrorist Actions and Sabotage: Medium risk. However, we need to be diligent in monitoring this exposure.

Disaster Planning – Preparation

In order to facilitate recovery from a disaster which destroys all or part of the server room, certain preparations have been made in advance. This document describes procedures for a quick and orderly restoration of facilities in both the TMA Corporate environment and our SaaS infrastructure.

The following topics for disaster preparation include:

- Disaster Recovery Planning
- Recovery Facility
- Replacement Equipment
- Backups
- Disaster Recovery Physical Plan

Disaster Planning:
This document along with the Information Policy Framework (primarily the: Business Continuity Policy and Information Security Incident Management Policy) are the backbone of the Disaster Planning.

Recovery Facility:
TMA has all data (both client and TMA corporate data) backed up. WebTMA utilizes multiple forms of backups to protect client data: client databases at the primary datacenter are replicated every to a secondary disaster recovery datacenter to protect critical client data. TMA Data is held at the corporate facilities and backed up to an offsite datacenter daily.

Replacement Equipment:
TMA has a contract with Dell for up to 24-hour replacement of equipment.

Backups:
All data is backed up on a consistent basis.

Disaster Recovery Physical Plan:
The Physical Plan will be held by all members of the BC/DR Team (as defined in the Business Continuity Plan).

Disaster Plan - Activation

The Chief Executive Officer (Recovery Manager) sets the plan into motion. If this individual is not available, the responsibility is automatically delegated to the Chief Security Officer. Early steps to take are as follows:

- The Recovery Manager should retrieve the Physical Disaster Recovery Plan in both printed form and in digital form. Copies of the plan should be made and handed out at the first meeting of the Recovery Team which is made up of the BC/DR Team.
- The Recovery Manager is to appoint the remaining members of the Recovery Team to their responsibilities. This should be done in consultation with available members of Recovery Team based on their skill sets. The Recovery Manager’s decision about who sits on the Recovery Management Team is final, however.

- The Recovery Manager is to call a meeting of the Recovery Management Team at either the Downtown Tulsa Hyatt Hotel or another designated alternate site. All relevant individuals, even if not on the Recovery Management Team should be invited to this meeting. The following agenda is suggested for this meeting:
    - Each member of the team is to review the status of their respective areas of responsibility.
    - After this review, the Recovery Manager makes the final decision about where to do the recovery. The designated facility is the Downtown Tulsa Hyatt Hotel. If this facility is not available for any reason, the Recovery Manager is to declare emergency use of another facility.
    - The Recovery Manager briefly reviews the Disaster Recovery Plan with the team.
    - Any adjustments to the Disaster Recovery Plan to accommodate special circumstances are to be discussed and decided upon.
    - Each member of the team is charged with fulfilling his/her respective role in the recovery and to begin work as scheduled in the Plan.
    - Each member of the team is to review the makeup of their respective recovery teams. If individuals key to one of the recovery teams is unavailable, the Recovery Manager is to assist in locating others who have the skills and experience necessary, including locating outside help from within the organization or outside vendors.
    - The Recovery Manager should set the schedule of the next meeting of the Recovery Management Team. It is suggested that the team meet at least once each day for the first week of the recovery process.
- The Recovery Management Team members are to immediately start the process of contacting the people who will sit on their respective recovery teams and call meetings to set in motion their part of the recovery.
- The Recovery Manager is responsible for immediately setting up the designated Recovery Control Room at the Downtown Tulsa Hyatt Regency Hotel for occupation and use by the Recovery Management Team. This includes the immediate relocation of any personnel occupying the room. The baseline facilities for the recovery room:
    - Office desks and chairs
    - Telephones
    - Computer Workstation (including data service)
    - Printer
    - Copier/Fax Machine
- Mobile communications will be important during the early phases of the recovery process. This need can be satisfied using cellular telephones.

Equipment, Assessment, Protection & Salvage

The Recovery Manager (with assistance from the Recovery Team) will need to assess the damage, protect any valuable assets and determine what can be salvaged.

Protection: It is extremely important that any equipment, media, paper stocks, and other items at the damaged primary site be protected from the elements to avoid any further damage. Some of this may be salvageable or repairable and save time in restoring operations.

- Cover all computer equipment to avoid water damage.
- Cover all undamaged paper stock to avoid water damage.
- Ask the police/security guards at the primary site to prevent looting or scavenging.

Media:
The media on which our data is stored is priceless. Although we retain backups of our disk subsystems and primary application systems off-site, media located in the server room area contain extremely valuable information. If the media has been destroyed, such as in a fire, then nothing can be done. However, water and smoke damage can often be reversed, at least good enough to copy the data to undamaged media.

After protecting the media from further damage, recovery should begin almost immediately to avoid further loss.

Salvage Equipment:
As soon as practical, all salvageable equipment and supplies need to be moved to a secure location. If undamaged, transportation should be arranged through the Recovery Manager to move the equipment to an appropriate Cold Site, or to another protective area (such as a warehouse) until the Cold Site is ready.

Take great care when moving the equipment to avoid damage.

If the equipment has been damaged, but can be repaired or refurbished, the Cold Site may not be the best location for the equipment, especially if there is water or fire damaged that needs to be repaired. Contractors may recommend an alternate location where equipment can be dried out, repainted, and repaired.

Inventory:
As soon as practical, a complete inventory of all salvageable equipment must be taken, along with estimates about when the equipment will be ready for use (in the case that repairs or refurbishment is required). This inventory list should be delivered to the Recovery manager for the Recovery Team to assess. A complete list of disaster recovery hardware and supplies must be prepared to begin the recovery process.

Emergency Procurement:
The Recovery Manager will be responsible for procuring (based on data provided by the Recovery Team) any equipment or supplies necessary to bring operations back to an acceptable level. The Recovery Manager will work in coordination with the Administrative Team in making certain purchases can be made with current suppliers or alternative vendors.

Platform Recovery Procedures

This portion of the plan documents a list of platforms/servers to be restored at the recovery facility. All platforms/servers require server hardware, operating system, application service, security policy, network connectivity, controlled air conditioning, and power conditioning. The goal is to only provide recovery productions servers. Test servers will take lower precedence.

List of Platforms/Servers to Recover

- Active Directory Services Domain Controllers
- Database Servers
- Web Servers
- Reporting Services Servers
- Business Critical Servers (Administration/Development)
- File and Print Servers
- Test Database Servers
- Test Web Servers

Application Recovery Procedures:
Once the platform system software and subsystems are operating correctly, the task of preparing the remaining end-user applications can begin. Each platform will have a unique recovery road to follow. In some cases, there may be very little to do except for general testing. In other cases, considerable analysis and data synchronization work will likely be required.

The Applications Recovery Team will be responsible for carrying out this phase of the recovery. Each application area will require a review. This review should be conducted by an individual familiar with the application while working closely with an application user representative.

Items to be considered should include:

- Review of the application documentation concerning file and database recovery.
- Review the status of files and databases after the general platform recovery processing is complete.
- Identify any changes to bring the application to a ready for production status.
- Identify any areas where the application must be synchronized with other applications and coordinate with those application areas.
- Identify and review application outputs to certify the application ready for production use.

Maintaining the Plan

The plan will be routinely evaluated once a year. All portions of the plan will be reviewed by the Chief Executive Officer, the Chief Security Officer and other relevant personnel o. In addition, the plan will be tested on a regular basis and any faults will be corrected. The Chief Security Officer has the responsibility of overseeing the individual documents and files and ensuring that they meet standards and are consistent with the rest of the plan.

Who the Policy Applies to

The policy applies to all users of Company information. Users include all employees, consultants, suppliers, or contractors working for or on behalf of the Company and any other person permitted to have access to TMA's IT and digital resources including visitors.

Where the Policy Applies

This policy applies to all locations from which Company information is accessed. This includes: TMA's Corporate offices, remote access from client sites and home use.

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 Technology Policy**
- **Network Administrative Security Policy**
- **Data Encryption Policy**
- **Monitoring and Logging Policy**
- **Business Continuity Policy**

VII. Update Log

June 1, 2015: Policy issued.

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