[FIRM NAME]
DISASTER RECOVERY POLICY

Overview

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives [Firm Name] a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered.

Purpose

This policy defines the need for management to support ongoing disaster planning for [Firm Name].

Scope

This policy applies to the management and technical staff of [Firm Name].

Contingency Plans

The following contingency plans must be created:

- **Computer Emergency Response Plan**: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
- **Succession Plan**: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
- **Data Study**: Detail the data stored on the systems, its criticality, and its confidentiality.
- **Criticality of Service List**: List all the services provided and their order of importance. It also explains the order of recovery in both short-term and long-term timeframes.
- **Data Backup and Restoration Plan**: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.
- **Equipment Replacement Plan**: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
- **Mass Media Management**: Who is in charge of giving information to the mass media? Also provide some guidelines on what data is appropriate to be provided.

Placing Plans into Action

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster plan. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

Updating Plans

Review all plans annually so changes in [Firm Name]'s situation can be incorporated.

Enforcement

Any employee that violates this policy may be subject to disciplinary action up to and including termination of employment.

Definitions

- **Disaster**: Any event that could likely cause serious disruption of the Information Technology systems, including, without limitation, weather events, power events, or acts of terrorism.

Revision History

A history of revisions to this Plan will be maintained by [Name or Position].

[FIRM NAME]
DISASTER RECOVERY PLAN

Document Control

Version	Date	Name	Description
V1.0			

Confidentiality

All information contained in this document is confidential to [Firm Name] and contractors and service providers supporting its operations. This document is intended for use only within [Firm Name]. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language or other language without the permission of [Firm Name].

Introduction and Executive Summary

The purpose of this Disaster Recovery (DR) Plan is to describe the technical activities instituted by [Firm Name] to ensure that the Information Technology (IT) systems meet the recovery protection objectives (RPOs) and recovery time objectives (RTOs) defined by the business to ensure continuity of its operations, the safety of its employees, and physical and intellectual assets in the event of a critical incident at its operational facility.

The plan outlines the Disaster Recovery plan for Information Technology once the business has declared a critical incident that impacts the computer facility.

Publication and Distribution Strategy

This plan should be reviewed after the annual Disaster Recovery Test, described in a later section of this document, or whenever any pertinent data has changed, whichever comes first. The plan should then be updated as needed, based on the test results and/or changes in key data, and re-published.

After publication, the plan should be distributed to all employees in soft copy. Additionally, a hard copy should be printed by each member of the Crisis Management Team (CMT) and stored in an easily accessible place (such as in their home or automobile), away from the normal operational facility, so as to be easily retrieved at a time when access to the operational facility is restricted or impossible.

IT Crisis Management Plan

- **Roles and Responsibilities of the IT Crisis Management Team**

Name	Role	Responsibility	Office Phone	Mobile Phone
	Business DR Lead			
	DR Lead			
	Backup DR Lead			

- **Emergency Contact Information**

Name	Address, if applicable	Phone	Contact
Fire/Police/Ambulance		911	
Police Non-Emergency			
Key Vendors			
Internet Provider(s)			

Strategies

- **ALERT PHASE – A Crisis Is Discovered**
  - A crisis is defined as any unplanned event that significantly threatens the health and well-being of [Firm Name]'s employees or assets, causes operational disruption, physical or environmental damage, or harm to the company's public image or reputation.
  - For the purpose of this plan, crises can include, but are not limited to:
    - natural disasters;
    - fires or explosions with damage;
    - life-threatening injuries;
    - hazardous material release; or
    - major utility failure.
  - When a crisis is discovered, the person discovering the crisis will promptly notify all members of the CMT. When reporting an incident to the CMT, the reporter should be prepared to answer the following questions:
    - What appears to have happened?
    - Are there any injuries?
    - When was the incident detected? (day, time)
    - Who is involved? (Emergency Response Team, other associates, etc.)
    - What is being done, why, and by whom?
    - Who is aware of the crisis, and who else needs to be notified?
  - After initially assessing damage to their areas, members of the CMT will assemble at the [Designated Location]. In the event the primary Command Center is not accessible, all members of the CMT will assemble at [Designated Alternate Location].

  - The DR Lead and Backup DR Lead will then determine, based on the initial damage assessment, whether or not to implement the Disaster Recovery Plan.

- **CRISIS PHASE – The Disaster Recovery Plan Is Implemented**
  - The primary alternate site from a DR perspective will be for all employees to work from home or an alternate operating location of [Firm Name].
  - A secondary alternate site may be designated at some point during a crisis by the DR Lead or designee.
  - During a crisis, all members of the CMT will:
    - Maintain an activity log to track events relating to their role during the crisis period.
    - Monitor responses from emergency service agencies and notify other personnel, as needed.
    - Revise damage assessment as the situation develops and assist the DR Lead and Backup DR Lead, as needed.
  - The DR Lead and Backup DR Lead will:
    - Notify the Business DR Lead or Corporate Administration Team of the implementation of the DR Plan.
    - Revise the overall damage assessment, as new information develops, and determine the appropriate level and method of response.
    - Provide periodic communications reporting changes in the status of the crisis.
    - Work with the Business DR Lead to decide whether to close the normal operational facility temporarily or indefinitely, if justified.
    - Decide when to open the facility on a limited basis or a full service basis once the effects of the crisis have been remedied.
    - If necessary, decide in consultation with the Business DR Lead whether to move operations to an alternate facility.
- **RECOVERY PHASE – Normal Operations Are Resumed**
  - During Recovery, all members of the CMT will furnish an IT Crisis Management report to the Business DR Lead.
  - The DR Lead and Backup DR Lead will:
    - Notify Business DR Lead regarding all IT Crisis Management and Recovery efforts.
    - Address any questions employees have about what to expect in the future for IT.
    - Provide a consistent “core message” about what has occurred.
    - Capture lessons learned from the experience and changes to be made in policies and procedures.

IT Disaster Recovery Plan Activities

In the event of a disaster that prevents access to ATG REsource® and support data processing systems at its processing centers, [Firm Name]’s return time objective (RTO) is to return to a minimum level of processing capability within [#] hours of a major incident. Data recovery protection objective (RPO) or maximum data loss due to a major outage is [#] hours.

In order to protect itself from the possible loss of data in its electronic records, [Firm Name] performs the following:

- All backup media is to be stored offsite using a secure transport.
- Application and database environments have the following backups:

  [Describe backups.]

Offsite restoration of the most recent backup has been tested and verified, and could occur at any [Firm Name] location with network connectivity.

- **Detailed IT Recovery Activities**

  [Describe recovery activities to bring up the IT environment.]

Organizational Test and Maintenance Plan

The CMT will conduct a test of this DR Plan on an annual basis or more frequently, as directed by the Business DR Lead.

- **Purpose of the test:**

  Annual testing allows the organization to link together and validate individuals' and teams' actions under the DR Plan.

  All testing instills confidence in the participants, which will ensure a more effective response to an actual emergency.

  Client requirements and industry regulations often mandate testing.

  Testing provides the most realistic and effective training possible.

  Not testing creates the risk that, in an actual emergency, our plans will fail.

- **Goal of the test:**

  Test the accuracy and effectiveness of the DR Plan components in order to provide input for continually improving the plan.

  The goal of the test is not to measure whether or not the Plan "passes" or "fails." Failure of the plan components is a positive result since failure provides the most valuable source of input to improve the plan.

- **Test Scenario:**

  Prior to the actual test exercise, a scenario should be agreed upon by the CMT, including a "disaster" to be simulated during the exercise, a conference room or other location to be designated as the "Command Center," and other easily accessible location(s) to serve as the "alternate site(s)" for the individual process Contingency Plans to be tested.

  The Backup DR Lead or other designated member of the CMT tests the contact information contained in the IT Crisis Management section of this plan by contacting all other members of the CMT to inform them of the simulated "disaster," clearly identifying it as a "Test Exercise," and notifying them that a meeting of the CMT will shortly be convened. This can be followed up by testing the other Emergency Contact Information in that section of the Plan.

  The CMT meets at the Command Center designated for the exercise. Members are asked to provide simulated damage assessments and the designated CMT leader will make the decision to implement the DR Plan.

  Restore most recent back-up tape at the designated alternate site.

  Test data generated manually during exercise of the Process Test Scripts will not be re-entered into the system as it would after an actual disaster.

  All test participants record their activities, as well as their observations and any issues that arise.

  CMT members re-convene to review the results, issues, and observations, and assign action items to prepare the official test results.

  The official test results should contain improvements that will be made to the Plan, lessons learned from the exercise, and overall evaluations and observations.

  Once the official test results are prepared, they are distributed to all participants and presented to the Business DR Lead by the CMT leader.

Glossary of Business Continuity Terms

- **Alert**: Notification that a potential crisis exists or has occurred; direction to stand by for possible implementation of emergency measures.
- **Alternate Site**: A designated location to be used to conduct business when the primary facility is not accessible.
- **Business Continuity Planning**: The process of developing advance arrangements and procedures that enable [Firm Name] to respond to a crisis in such a manner that critical business functions continue with planned levels of interruption or essential change.
- **Business Impact Analysis**: The process designed to identify critical business functions and workflow, determine the qualitative and quantitative impacts of a disruption, and to prioritize and establish recovery time objectives.
- **Call Tree**: A document that graphically depicts the names and contact information for persons to be called in the event of a crisis.
- **Command Center**: A physical or virtual facility located outside of the affected area used to gather, assess, and disseminate information and to make decisions regarding the response to a crisis.
- **Contingency Plan**: The steps to be followed in order to conduct a business process without access to the normal operational facility and tools.

- **Crisis**: A critical event, which, if not handled appropriately, could negatively impact [Firm Name]'s profitability, reputation, or ability to operate; the period of time during which a Business Continuity Plan is implemented.
- **Crisis Management Team (CMT)**: The key role players responsible for Business DR, who implement [Firm Name]'s response to a crisis in an effective, timely manner, with the goal of avoiding or minimizing damage to [Firm Name]'s ability to operate.
- **Disaster Recovery (DR) Plan**: The steps needed to be taken to restore [Firm Name] to an acceptable operating condition.
- **Operational Facility**: The place from which business is normally conducted (i.e., the office).
- **Processor**: The employee who conducts or exercises the steps of one of the business processes.
- **Recovery**: The period of time when steps are taken to restore business processes and support functions to operational stability following a crisis.
- **Recovery Point Objective (RPO)**: The point in time to which systems and data must be recovered after an outage.
- **Recovery Time Objective (RTO)**: The period of time within which systems, applications, or functions must be recovered after an outage.

APPENDIX

The appendix includes diagrams and supporting documentation to support the Disaster Recovery Plan.