LADENBURG THALMANN & CO. INC.

Business Continuity Plan / Business Recovery

September, 2019

I. Business Recovery Overview

A. Purpose

The Business Continuity Plan (BCP) contains the information and procedures that will be needed to recover business operations if a disaster should occur. This plan is intended to assist in ensuring our ability to provide our services with a minimum of disruption and with full accuracy in the event of a disaster.

In addition to satisfying the requirements of FINRA and the SEC, this plan is intended to help Ladenburg Thalmann & Co. Inc. (LT&Co.) prepare personnel to respond quickly and effectively in a recovery situation and to minimize risk to the company, its customers, stockholders and reputation. Maintaining the integrity of our customer files and company files is of great importance and should be accomplished by following this plan.

B. The Success of the Plan

The success of the Business Continuity Plan (BCP) will depend upon the following pre-disaster activities:

- The BCP is updated and tested periodically
- The BCP is updated after any major changes occur, such as the implementation of a new application processing system, expansion of the building or business or major alterations in the organizational structure of the organization
- All Team Leaders are trained thoroughly as their roles with the recovery effort
- Critical files are saved and stored off-site daily
- Essential software is saved and stored off-site immediately following major software or hardware changes
- The BCP, critical forms, and supplies are stored off-site in a secure location and are immediately available
- Training of all employees in evacuation and emergency procedures is preformed, including instruction on shutdown procedures.

C. Objectives

The objective of this BCP is to provide the necessary information and procedures to

- Protect the lives of customers and employees
- Reduce the magnitude of loss by reducing the time needed to recover from a disaster
- Ensure the ability to recover critical data in a timely manner
- Assure that LT&Co. can function until the primary site is repaired or replaced
- Prepare personnel to respond quickly and effectively in a recovery situation
- Minimize risk to LT&Co.'s clients and reputation

D. Business Impact Analysis & Risk Assessment

i. Business Impact Analysis

A Business Impact Analysis (BIA) will be conducted initially and then reviewed annually. Executive staff in each line of business will contribute to the BIA. Every year, any new risks will be identified and addressed in the BIA. Senior Management will review and approve the BIA each year.

ii. Risk Assessment Process

One of the first tasks to be performed by LT&Co. is to identify the potential threats to our firm and the impact these risks could have on our business. Potential threats to the organization are classified in two categories – Internal Threats and External Threats.

- *Internal Threats* affect only LT&Co.'s ability to communicate and transact business, such as a fire in one of its offices.
- *External Threats* prevent LT&Co.'s operations, such as a terrorist attack, a city flood, or a wide-scale, regional disruption. Our response to an external threat relies on wide area infrastructure being in place

Potential internal threats assessed include but not limited to:

- Internal Fire
- Active Shooter
- Unauthorized Modification of Software or Hardware

Potential external threats assessed include but not limited to:

- Hazardous weather (tornado, ice storm, blizzard, etc.)
- External Fire
- Terrorist attack
- Earthquake
- External Explosion
- Pandemic

iii. Existing Disaster Prevention Measures

The following disaster prevention measures are currently in place at LT&Co..

- Emergency lighting is in place throughout the facility
- Fire Extinguishers are in place throughout the facility
- The network servers are on UPS and/or backup generators
- The network servers are backed up daily to DR

iv. Critical Third-Party Suppliers

All critical third-party providers for firm operations should be identified and the list reviewed and updated annually. Contact names and numbers for suppliers should be documented and securely stored.

v. Operational Assessments

- Operational Risk
- In the event of a threat, we will immediately identify any available means by which we may communicate with our clients, customers, employees, and other critical business constituents. Although the impact of a threat will largely dictate the available means of alternative communication, the communications options that we will employ include telephone, voice mail, e-mail, and the Ladenburg Thalmann & Co. Inc.'s (LT&Co.) Company website.
- In addition, we will retrieve our key activity records
-

E. Disaster Escalation Levels:

Outage Time Period	Criticality / Escalation Level	Interruption Description	Recovery Plan
0 – 8 hours	Level 1	Problem	Used when the interruption is estimated to be 8 hours or less. Requires some modification to the scheduled work load. Use normal system management procedures to recover.
8 – 24 Hours	Level 2	Emergency	Used when the interruption is estimated to be between 8 – 24 hours. Modifications will be made to the scheduled work load to permit the highest priority application systems to run as soon as possible. Partial or full mobilization of the Business Recovery Plan may be necessary. Use system management procedures and BCP to recover.
24 + hours	Level 3	Disaster	Used when the interruption is estimated to be 24 hours or longer. Full mobilization of the Business Recovery Plan is declared. Use BCP to recover.

Distribution of the Plan

One complete copy of the Business Continuity Plan (BCP) is kept at an off-site location and one complete copy should be kept on-site. A list with the location of each copy should be kept at Ladenburg Thalmann & Co. Inc (LT&Co.), as well as with the copy that is kept off-site. BCP can also be emailed. The Business Continuity Plan should be updated with the location of each copy of the plan.

G. Testing and Maintaining the Plan

i. Testing

The Business Continuity Plan (BCP) will be tested periodically to ensure the feasibility of the plan and to demonstrate that Ladenburg Thalmann & Co. will be able to recover from a disaster.

This testing plan will be accomplished in the following ways:

- A combination of a checklist test and a structured walk-through of the plan will be conducted with management and team leaders. Using a checklist and performing a walk-through of the plan will ensure adequate supplies and critical records are stored off-site, employee emergency contact information is current, and copies of the plan and other necessary information is available.
- A simulation of a disaster will be performed, which will involve all employees. This will provide an opportunity for team leaders, management, and support staff to practice and understand the Business Continuity Plan.

This testing of the plan will be performed periodically. All employees will be trained and tested on evacuation annually to ensure employees remember the procedures. All new employees must be trained. The Management Team is responsible for this task.

All security equipment (including fire/smoke detection systems) will be tested and/or inspected periodically. A third-party vendor is responsible for this task.

ii. Maintenance

Ladenburg Thalmann & Co. (LT&Co.) will annually review and revise the Business Continuity Plan and incorporate any required document maintenance and other changes that are needed. The Plan will then be reviewed by the Management Team for approval.

Items likely to cause maintenance are:

- Personnel Changes
- Employee address or telephone changes

- Equipment changes or upgrades
- Changes in vendors
- Changes in processing arrangements
- Changes in Critical documents and supplies
- Departmental changes what will result in modification to recovery procedures
- Modifications to the testing procedures

iii. Departmental Disaster Recovery Plans

Additional Departmental Disaster Recovery Plans are maintained in separate documents that are maintained by the individual departments. The management, maintenance, and testing of these documents is the responsibility of the department managers and IT departments and will be required as part of the documentation review for the annual LT&Co. Business Continuity Plan Revision and Maintenance.

H. Business Recovery Teams

Eugene Kvasov	IT Department	212 409-2020	ekvasov@ladenburg.com
Alex Alvarenga	IT Department	212 409-3344	aalvarenga@ladenburg.com
Russel Rogers	Cybersecurity	212 409-2082	rrogers@ladenburg.com
Robert Mateicka	Compliance	212 409-2021	rmateicka@ladenburg.com
David Rosenberg	CEO	212 409-2222	drosenberg@ladenburg.com
Rick Sonkin	BOM	646 432-6341	rsonkin@ladenburg.com
Maria Molino	LTAM	212 891-5236	mmolino@ladenburg.com
Kelly Fontanetta	HR	631 270-1619	kfontanetta@ladenburg.com

i. Brief Description of Team Leaders

The Management team members are the primary decision-makers. They are responsible for executing the Business Continuity Plan and setting goals and priorities. They will approve expenditures for equipment, services, and expenses for those traveling to alternate processing sites, and other expenses that occur as a direct result of the recovery effort. They will also make decisions for issues that are not addressed in this plan.

a. Team Leaders/Management

The team leaders will be responsible for coordinating the recovery efforts the team.

These individuals will:

- Address issues not covered in this plan
- Contact team members, notifying them where and when to meet
- Assign and explain recovery responsibilities and tasks
- Monitor the progress of recovery tasks

- Work closely with other teams
- Educate team members on Recovery Responsibilities, prior to the occurrence of any situation which would call for the use of the Business Recovery Plan

b. Management Team

The Management Team will be responsible for the overall recovery effort of the organization if a crisis occurs. This team will review the damage information and determine if the situation warrants that a disaster be declared.

Management Team responsibilities include:

Pre-Disaster

- Training employees on Business Recovery Plan
- Conducting training for new employees on emergency procedures

During Disaster

- Disaster Declaration
- Coordination of the overall recovery effort
- Public Relations, including release statements to the press
- Making decisions regarding unplanned events
- Updating employees, executive management stakeholders
- Oversee the repairs and reconstruction
- Oversee the purchase of equipment and services needed for recovery

Post-Disaster

- Assess overall performance of teams during recovery process
- Assess overall effectiveness of the Business Recovery Plan
- Assess overall effectiveness of Processing vendor(s)
- Modify existing recovery procedures, as necessary

c. Damage Assessment

Ladenburg Thalmann & Co. Inc. (LT&Co.) will review the damage caused by the situation that has occurred, recording the information.

Damage Assessment responsibilities include:

Pre-Disaster

- Verify that all equipment, vendor, and facility information has been included in the Business Recovery Plan
- Be familiar with the facility/facilities

- Review and analyze test results
- Be familiar with the Business Recovery Plan

During Disaster

- Perform Damage Assessment
- Generate a report indicating the specific areas affected by the disaster

Post-Disaster

- Asses overall effectiveness of the disaster revovery process
- Assess overall effectiveness of the Business Recovery Plan
- Modify existing disaster recovery procedures, as necessary

d. Business Recovery Team

The Business Operations Recovery Team is responsible for overall business administrative functions throughout a recovery effort. This team works directly with the HR representative and the management team.

Responsibilities include, but are not limited to:

Pre-Disaster

- Contact manufactures and suppliers to make necessary advance preparations for emergency response, repair, and replacement
- Establish working relationships with other resources, such as civil authorities, facility owners, insurers/agents, salvage specialists, etc.
- Confirm with department heads that key employees are cross-trained

During Disaster

- Purchasing
- Overseeing Insurance Issues
- Personnel issues
- Finding a site suitable for the Recovery Command Center if the *planned location* is not available
- Ensure that the necessary equipment, supplies, and services are ordered and delivered in a timely manner
- Salvage equipment and the facility
- Arrange for the removal of damaged equipment
- Other Administrative Functions, including Recovery Management Documentation
- Establishment of Work Areas for their respective departments at the Recovery Command Center

- Recovery of processing for each of the departments listed above, including working with each department to recreation of work that was in progress at the time the Disaster occurred
- Performing departmental functions as usual, whenever possible
- Maintaining high customer service standards from the Recovery Command Center

Post-Disaster

- Assess overall effectiveness of the Business Operations process
- Assess overall effectiveness of the Business Recovery Plan
- Modify existing Administrative Team recovery procedures, as necessary

Business Recovery Team

The Business Recovery Team is responsible for establishing the day-to-day connections and network support both for internal business operations and the external employees at LT&Co. The Business Recovery Team will work directly with all other team leaders to ensure all work can be processed.

Responsibilities include but are not limited to:

- Any critical IT functions that can be done, either automatically or manually
- Daily reports
- Backup & Recovery
- Network connectivity
- Communications
- Commissions File Access
- Connect Functionality
- Revenue Center Access
- Fee reports

Pre-Disaster

- Annually, request a recovery test report from third-party vendors (as available)
- Annually perform recovery test
- Annually test the DR site, disaster recovery programs
- Test manual Mission Critical Functions
- Maintain team training
- Compile and maintain list of all tasks that are critical

During Disaster

- Contact Management
- Contact all IT operations third party vendors and system contractors
- Evaluate, assess, and resolve connectivity issues
- Communicate outage statuses and updates to management and staff
- Reestablish IT systems, IT network, and IT security functionality
- Initiate offsite IT recovery procedures (as needed)

Post-Disaster

- Assess overall effectiveness of the Computer Operations recovery process
- Assess overall effectiveness of the Business Recovery plan
- Modify existing Computer Operations recovery procedures, as necessary

Recovery Facilities and Processing Sites

i. Designated Meeting Place and Supervisor

The designated meeting place is the site at which the employees should meet if they must evacuate the building. Employees should evacuate to this site immediately and wait for a head count and further instructions. Completing the head count, the Department Supervisor will be responsible to determine which employees are missing and try to account for them and then report this information to the Management Team.

Designated Meeting Place for Ladenburg Thalmann & Co. Inc. (LT&Co.) is the southeast corner 375 Park Ave. New York, N.Y. (Park Ave. & 52nd St.)

I. Critical Services and Recovery Priorities

Recovery operations are prioritized based on LT&Co.'s needs. These priorities are:

Priority 1	• Secure and setup a location • Establish/re-establish phone services • Server setup and access	• Critical application access • Re-direct incoming number(s) • Domain Controller operation • Database access
Priority 2	• Provide remote access	• Provide remote access procedures
Priority 3	• All remaining services	

J. Emergency Instructions

i. Evacuation Policy

Ladenburg Thalmann & Co. (LT&Co.) has established an "Evacuation Policy" which states:

1. Evacuation of the building will be initiated by either the sounding of the fire alarm, or by verbal communication from the Management Team.
2. All employees should immediately proceed to the nearest exit and walk to the Designated Meeting Place.
    a. The Designated Meeting Place is located at Park Ave. & 52nd. St.
3. Should you be aware of anyone with a walking disability in your vicinity, please take responsibility for assisting that person out of the building.
4. Out of the building, proceed to the Designated Meeting Place.
5. Do not go back into the building until advised by the Management Team or the Fire or Police Departments.
6. Do not leave the premises without Management Team advisement.

ii. General Emergency Policies

1. The first and most important rule in an emergency is that the protection of all personnel must be the priority. Protection from injury will take priority over all other issues.
2. If possible (if there is no danger or injury) the following should be attempted to salvage or move to a safe location those items critical to recovery:
    a. Vital records located in LT&Co.'s Network servers are backed up and stored in multiple sites. If a disaster occurs such as fire, water damage, etc., (hard) original client documents, legal documents would be destroyed. LT&Co. saves all documents and legal documents to appropriate drives.
    b. Network Equipment
    c. The most current hard-copy reports

3. Notify Recovery Personnel
    a. Management
    b. Business Recovery Teams

iii. In Case of Power Failure

1. LT&Co. has all critical systems on UPS to keep business operations moving forward. Not all computers and non-critical systems are on UPS and these systems will lose power in the event of an outage. The Miami Fl. location every computer is UPS.
2. Electronic key entry is not on the generator power and will release all doors in the case of power loss.

iv. In Case of ISP (Internet Service Provider) Failure

1. In the event of ISP failure, LT&Co. has a backup ISP in place to maintain network connection.

v. In Case of Equipment Failure

1. Procedures for equipment failures depend on the type of equipment failed and the length of down time for that equipment.
2. Log the failure and notify Management so that maintenance can be scheduled as soon as possible. Be sure to document any error messages and/or details that might be required for repair.

vi. In Case of Fire

1. Use a fire extinguisher to try to contain the fire, if possible.
2. If the fire extinguisher is not sufficient to put out the fire, call the fire department using the number 911.
3. Begin the evacuation policy to the Designated Meeting Place. If the smoke is thick, drop to the floor and crawl to the nearest exit. Cover your mouth to avoid inhaling smoke and gases.
4. Close all exterior office doors if possible.
5. Check all non-working areas to make sure all personnel have been alerted (break room, restrooms, etc.).
6. Evacuate the building and make your way to the Designated Meeting Place and wait for further instructions.
7. At the Designated Meeting place the Management Team will attempt to account for all personnel.
8. The Disaster Recovery Administrator will contact all other employees, if they are not at the Designated Meeting Place.

vii. In Case of Severe Thunderstorms/High Winds/Tornado/Hurricane

1. Guide and assist in moving employees and customers to a safe place, such as an inside hallway. Stay away from glass, such as windows and mirrors. Get under a piece of sturdy furniture and use your arms to protect your head and neck.

The remaining steps should be done only if time permits!

2. End any work running on PC's and log off. Any equipment not attached to the UPS should be unplugged. All CD's and thumb drives should be placed in a fireproof safe.
3. Store all files, records and other items in a fire proof file cabinet.
4. Check all non-working areas to make sure all personnel have been alerted (break rooms and restrooms).
5. If necessary, when it's safe, evacuate the building. Go to the Designated Meeting Place and wait for further instructions.
6. At the Designated Meeting Place, the Management Team will attempt to account for all personnel.

7. If people have been injured or property harmed by the severe weather, the Disaster Recovery Administrator will contact all other employees, if they are not at the Designated Meeting Place.

vii. In Case of Bomb Threat

1. Follow the instructions provided by this Business Continuity Plan.
2. Leave all doors and windows open.
3. Check all non-working areas to make sure all personnel have been alerted (employee break room, rest rooms, etc.).
4. Leave the building. Go to the Designated Meeting Place and wait for further instructions.
5. At the Designated Meeting Place, the Management Team will attempt to account for all personnel.
6. Dedicated personnel will contact employees not at the Designated Meeting Place.
8. Notify the proper authorities.

viii. In Case of Widespread Illness or Pandemic

Should a pandemic occur, management will, after consultation with knowledgeable health officials, implement the following steps, as deemed necessary:

1. Employees with job duties that can be accomplished by telecommuting will be encouraged to work from home unless they have been cross-trained to work in place of an employee who is ill.
2. The emergency sick leave policy shall be implemented. Supervisors will be instructed to send and keep employees home if they exhibit symptoms of the illness, working from home if practical.
3. Team members will contact their key vendors to determine the impact of the outbreak on their operations and its effects on our ability to perform our daily functions, and they will communicate the results to management.
4. Department heads will monitor staffing levels for departments and assisting in finding ways to maintain critical operations considering any staffing shortage. Telephone and other lines of communication must be routed to a location or locations where they will be staffed by employees so attempts do not go unanswered.
5. Department heads are to implement the employee contact plan to ensure that all employees are kept informed of developments as they occur, including employees who remain at home.

ix. In Case of Suspicious Letters or Packages

Personnel should be instructed that if they receive a suspicious letter or package, they should not tamper with it. The suspicious item should be isolated, and Management should be notified.

Suspicious features include:

- Excessive weight or size
- Springiness in the top, bottom or sides
- Wires, tin foil or strings protruding or attached
- Peculiar odor
- Uneven balance
- Excess postage
- Mismatching of name and title
- Handwritten or poorly typed address and misspelling of common words
- No return addresses
- Visual distractions
- Soiled or stained packages
- Unusual markings

If you are suspicious of a mailing and are unable to verify its contents:

1. Do not open the article.
2. Isolate the mailing and secure immediate area.
3. If Management issues an evacuation, guide and assist in the evacuation of any customers and employees from the building to the Designated Meeting Place.
4. Leave all doors and windows open.
5. Check all non-working areas to make sure all personnel have been alerted (employee break room, restrooms, etc.).
6. Leave the building. Go to the Designated Meeting Place and wait for further instructions.
7. At the Designated Meeting Place, the Management Team will attempt to account for all personnel.
8. The Disaster Recovery Administrator will contact anyone who is not at the Designated Meeting Place.
9. Notify the proper authorities.

x. <u>In Case of Active Shooter</u>

Personnel should be instructed in the most reasonable way to protect their own life. Remember that coworkers are likely to follow the lead of other employees and managers during an active shooter situation.

1. Evacuate If there is an accessible escape path, attempt to evacuate the premises. Be sure to:

- Have an escape route and plan in mind

- Evacuate regardless of whether others agree to follow
- Leave your belongings behind
- Help others escape, if possible
- Prevent individuals from entering an area where the active shooter may be
- Keep your hands visible
- Follow the instructions of any police officers
- Do not attempt to move wounded people
- Call 911 when you are safe
    - Information to provide to law enforcement or 911 operator:
        - Location of the active shooter
        - Number of shooters, if more than one
        - Physical description of shooter(s)
        - Number and type of weapons held by the shooter(s)
        - Number of potential victims at the location

2. Hide out If evacuation is not possible, find a place to hide where the active shooter is less likely to find you. Your hiding place should:

- Be out of the active shooter's view
- Provide protection if shots are fired in your direction (i.e., an office with a closed and locked door)
- Not trap you or restrict your options for movement
- To prevent an active shooter from entering your hiding place:
    - Lock the door
    - Blockade the door with heavy furniture
- **HOW TO RESPOND WHEN A N ACTIVE SHOOTER IS I N YOUR VICINITY**
    - If the active shooter is nearby:
        - Lock the door
        - Silence your cell phone and/or pager
        - Turn off any source of noise (i.e., radios, televisions)
        - Hide behind large items (i.e., cabinets, desks)
        - Remain quiet

    - If evacuation and hiding out are not possible:
        - Remain calm
        - Dial 911, if possible, to alert police to the active shooter's location
        - If you cannot speak, leave the line open and allow the dispatcher to listen

3. Act against the active shooter

- As a last resort, and only when your life is in imminent danger, attempt to disrupt and/or incapacitate the active shooter by:

- Acting as aggressively as possible against him/her
- Throwing items and improvising weapons
- Yelling
- Committing to your actions

II. APPENDIX 1

Bomb Threat Procedures Checklist and Guidelines

A. <u>Action to be taken by employee receiving the call</u>:

1. Make a special effort to continue the conversation with the caller. (A signal should be set Up to notify Management that a bomb threat is being received. They can take the necessary action to have the telephone company trace the call.)

2. **Stay calm. Do Not upset the caller. Do Not hang up.**

3. While the conversation is going on, Management should call the Police Department 911

4. Try to tape record the conversation if possible.

5. Try to keep the caller talking. Fill in the following:

   - Location of the bomb? _____

     _____
   - When is it set to go off? _____
   - Is it in the open? _____
   - Is it disguised? _____
   - KIND and SIZE of bomb? _____
   - How was the bomb brought into the building? _____

     _____
   - Why was it put there? _____

     _____
   - Note the following:
     - Sex of the caller _____
     - Name of caller _____
     - Race of caller _____
     - Accent _____
     - Voice Characteristics (drunk, stammer, lisp, etc.) _____

- _____
- Attitude of caller (calm, excited, nervous, etc.) _____

(7) Background noises? _____

_____

(8) Where is the caller calling from? _____

(9) Name of person who received the call _____

(10) Time and Date the call was received _____

6. Notify the Management Team immediately.
7. Evacuate the building
    - Have everyone assemble at the Designated Meeting Place
    - Leave all doors open
    - Evacuate through the main doors or fire exits
    - Do not run, running causes panic
8. The building should not be entered until all is clear and made known by the Police or Fire Department personnel.

Damage Assessment Worksheet

To be completed during the Damage Assessment Phase (and as necessary in other phases):

Location: _____

- Access to the building:
  - ○ Open access at (time): _____
  - ○ Limited Access (explain): _____
    _____
    _____
  - ○ Access denied at (time): _____
  - ○ By (authority) _____
  - ○ Of (organization) _____
  - ○ Until (expected access time time) _____
  - ○ No safety concerns
  - ○ Safety concerns (explain): _____
    _____
    _____
  - ○ No security concerns
  - ○ Security concerns (explain): _____
    _____
  - ○ Other concerns (explain): _____
    _____
    _____
- Structure:
  - ○ Walls
    - ▪ No visible damage
    - ▪ Visible damage (explain) _____
      _____
      _____

- Floors
  - No visible damage
  - Visible damage (explain) _____
- Ceilings
  - No visible damage
  - Visible damage (explain) _____

- Equipment:
  - Moved during disaster _____
  - Contaminated by smoke or soot: _____
  - Showing signs of electrical problems: _____
  - Other (explain): _____
  - Undamaged equipment: _____
  - Damaged but Repairable (explain): _____
  - Destroyed (explain): _____

- Other (explain): _____

_____

_____

- Utilities:
  - Lighting
    - Primary working
    - Not working (explain) :_____

_____

_____

    - Backup working
    - Not working (explain): _____

_____

_____

  - Heating
    - Emergency heating working
    - Not working (explain): _____

_____

_____

  - Cooling
    - Cooling working:
    - Cooling not working (explain): _____

_____

  - Ventilation
    - Working
    - Ventilation not working (explain): _____

_____

  - Plumbing
    - Plumbing Intact
    - Ruptures, leaks (explain): _____

_____

_____

- Other (explain): _____

_____

_____

- Services:
  - Access Control
    - Working
    - Not working (explain) _____

_____

_____

  - Fire protection
    - Sprinklers not activated
    - Sprinklers activated (explain): _____

_____

_____

  - Power
    - Working
    - Not working (explain): _____

_____

_____

- Uninterruptible power supply system:
  - Batteries
    - Working
    - Not working (explain): _____

_____

_____

  - Generators
    - Working
    - Not working (explain): _____

_____

_____

- Other power considerations
  - Working
  - Not working (explain): _____

    _____

    _____
- Circuit breakers and power cables
  - Not damaged
  - Damaged (explain): _____

    _____

    _____
  - Other (explain): _____

    _____

    _____

- Supplies:
  - Damaged but usable: _____

    _____

    _____
  - Destroyed: _____

    _____

    _____

Preparer of report: _____

Date of report: _____ Time of Report: _____

Damage assessment information provided by:

1. Name: _____ Title/Position: _____

2. Name: _____ Title/Position: _____

3. Name: _____ Title/Position: _____

4. Name: _____ Title/Position: _____

Critical Items Request Form

Critical Forms & Supplies

Location: Corporate
Department: _____

Person Making Request: _____ Date: _____

Instructions: To order supplies, indicate the quantity needed of each item.

Critical Equipment Request Form

Critical Equipment Needed

Location: Home Office

Person Making Request: _____

Date: _____

Instructions: To order equipment, indicate the quantity needed of each item.

Qnty	Ordered	Rcvd	Equipment	Make	Model	Description	Serial #	Vendor

HR Time Record Form

Employee Name: Title:

Social Security Number: Status: Full-time Part-Time

Department: Supervisor:

Date	Start Time	End Time	Regular Hrs.	Overtime Hrs.	Total Hrs.
		WEEKLY TOTALS			

Employee Signature: Date:

Supervisor Signature: Date:

Disaster Recovery / Network Service

Introduction

The scope of this document is to provide details as to how Ladenburg Thalmann & Co. Inc. (LT&Co.) deals with disasters and the recovery of network services, when impacted. The procedures in this document will need to be carried out in the event of a disaster.

An event can occur based on one of several scenarios. This could include the loss of electrical power or the loss of Internet connection at the site. This document will guide LT&Co. on how to perform disaster recovery.

Anticipation

We take several measures to prevent any down time. In the event of power loss, our Comm. room is always powered by an Uninterrupted *Power* Supply (UPS). The UPS stores power for about 15 minutes depending on the load the servers are using. During the first 5 minutes of these 15 minutes.
In Miami Fl., a standby generator will automatically begin to start up when power is interrupted. Before the power has been exhausted from the UPS units, the power is switched over to the generator via an Automatic Transfer Switch (ATF). The generator uses oil.

We have also taken precautions in the event that our Internet Service Provider (ISP) connection goes down. We use two Internet Service Providers. Our primary ISP is supplied by Cogent. The connection has a capability 1Gig for both upload and download transfers. In addition, there is a second TW line with a 50.00 Mbps capacity.

External Third-Party Services

In addition to the two Internet Service Providers stated above, we have other outside services that we have contracted. LT&Co. has contracted SPS for our inhouse phones which consist of PBX hosted on-premise. These phones are completely dependent on the Verizon T1 lines

EFax provides us with our facsimile services. When faxes are sent to us, they are emailed to us in an electronic format. This will continue to work provided we have an email server.

NFS offers clearing solutions, such as core processing, business continuity, reporting, and middle-office solutions. To place trades, open accounts and lookup client account information our employees and representatives use the NFS provided web site, www.wealthscape.com. NFS also provides our employees with back-office support via their telnet FBSI service. These sites are hosted on NFS's servers, and a SSO is provided to our reps via the Enterprise Platform.

We also host an off-premises web site www.Ladenburg.com. Through this site we are able to post messages to our employees for information and emergency notifications. The site is hosted on servers that do not reside on an LT&Co. network.

After the September 11th attacks, the SEC has required financial institutions to have a secondary (disaster recovery, DR) site replicating all services on the primary site. The site is suggested to be at least 200 miles away from the primary site. The site should be able to take over and assure that the business can continue to function without the primary site. LT&Co.'s DR server site is in La Vista NE. housed at the Securities America Inc. location.

Locations and Contacts

LT&Co.'s primary site is currently located in the Comm. room at 277 Park Ave. 26th floor, NY N.Y. 10172. The only LT&Co. employees that have access to the data center are Eugene Kvasov (Manager of IT Dept.) and Alex Alvarenga (IT Specialist).

The DR site is located at 12325 Port Grace Blvd. La Vista NE 68128. LT&Co. relies on Securities America Inc. (SAI) IT dept. employees for physical access to the DR Site. This location is monitored and accessible 24 hours, 365 days a year.

POST Disaster

We are going to assume that our ISP provider Cogent is down for this scenario. The following are the first few sequences of events that will occur in the event of a disaster. Depending on the day and time of day, some services that are down will be noticed first versus the others. Internally, if it is during operating hours (Monday – Friday 8:00 AM – 5:00 PM), our employees will notice that they cannot access the Internet.

Once they cannot reach us via telephone, they will try and send an email. The LT&Co. email servers will not be affected and will be available for the sending and receiving of messages.

Time Warner ISP will be utilized as a back-up.

No mission critical systems would be impacted.

If both ISP carriers Cogent and Time Warner are down LT&Co. will not have access to Internet and NFS. Other mission critical systems have dedicated lines and would not be impacted.

Employees requiring NFS access will be directed to other LT&Co. locations, Melville NY and Miami Fl. to conduct business.

Immediate Procedures for Communication

Public Notifications and Alerts

We need to communicate with our employees to let them know that we are aware of the problem and that we are working on a solution. Calling tree and notification via LT&Co. website will be utilized for advising employees of the current situation.

Phones Services

Verizon provides 2 dedicated lines
Windstream provides 2 dedicated lines (Trading)
Stage 2 (Inter-office dialing)

Web-Site Access

www.ladenburg.com hosted by Equisolve located in Florida.

Incoming Phone Call

If the downtime is during work hours, the main number 1 800 LAD-THAL will be operative.

Ideally there should be a person or group of persons that will be the skeleton crew for LT&Co.. There should be at least one person from each department as part of the group. The persons can be present or remote and should be ready to handle any questions our employees might have.

Redirection Via LT&Co. Provided Phone

The skeleton crew should be moved to an area where there is Internet access. The location

can be their individual homes, an employee's office or any location where an Internet hotspot exists. If they have physical access to a Local Area Network (LAN) connection, then they can plug in a notebook computer and log into the DR site via the VPN.

Redirection Via Personal Phone

If LT&Co. phones are unavailable, employees will utilize LT&Co. phones (previously provided) or their personal mobile phones.

Disaster Recovery Site Network Connections

LT&Co. uses VPN to connect to DR from New York City, Melville NY and Miami Fl.

Network Service Recovery and Switch Over

VPN is utilized.

Network.com Exchange Mail Server

LT&Co. uses Microsoft Office 365 as it's email provider. The primary Exchange mail server is hosted by Microsoft. Regaining access is dependent on end-user internet connectivity.

Windows Domain / DNS

The primary external DNS server is hosted at LT&Co.. Back-up DNS' is located New York City, Melville NY, Miami Fl. & LaVista NE.

SSNetwork.com and other sites

The corporate web site, Ladenburg.com, is hosted y Equisolve.

By following the above procedures, the most important and used LT&Co. network services will be back online. Depending on the time it takes to recover, from the disaster, additional different procedures might need to take place. If possible and needed, we can relocate servers to the DR site. Depending on the extent of the disaster, the DR site might need to be a new site permanently.