



SterlingRisk

Business Continuity Plan

Version Control

<u>Date of Revision</u>	<u>Reason for Revision</u>
04/10/2015	Initial re-write
06/15/2016	Updated Contacts, Risk Assessment and other logistical info
11/30/16	Updated Addendums to include new/updated info
07/10/17	Reviewed CMT members and updated Risk Assessment
12/13/17	Updated Addendums to include updated info
11/14/18	Updated Addendums to include new/updated info
10/22/19	Annual Review
03/05/20	Reviewed and updated Risk Assessment Chart
11/01/21	Updated to reflect move from 8x8 to Zoom for Phones
12/13/21	Updated Risk Assessment Chart included

SterlingRisk will shred any previous versions of this document due to privacy and confidentiality issues as well as routinely review and update this Plan to ensure data is current.

Table of Contents

Executive Summary	5
Objective/Purpose of the Preparedness Plan.....	5
Location of the Preparedness Plan.....	5
Definition of Crisis Management Team (CMT)	6
CMT Members, Roles & Contact Information	6
CMT Member Individual Responsibilities	8
Assumptions.....	10
Audience	10
Distribution	10
Maintenance	10
Risk Assessment	11
Critical Business Functions.....	Error! Bookmark not defined. 3
Communication Plan.....	17
Phone Recovery Template	18
*Employees Contact List – See myAgility	21
*Vendors Contact List – See myAgility	21
Evacuation Plan	22
Preparedness Plan Maintenance, Training, and Testing	23
Maintenance of Plan	23
Training Employees	23
Testing/Exercising of Plan.....	24
Suggestions for Tests/Drills.....	24
Additional Testing and Training Resources	27
Training and Testing Log.....	28
Recovery Procedures/Incident Response.....	I
Recovery Procedures	II
Power Recovery Overview	III
Power Recovery Process.....	IV
Space Recovery Overview	VI

Space Recovery Process	VIII
Technology Recovery Overview	IX
Technology Recovery Process	X
Connectivity Recovery Overview	XI
Telecom Recovery Process	XII
Communications Overview	XIII
Alert Notification Procedures	XIV
Recovery Checklists.....	XIIIIV
Winter Weather Recovery.....	XIV
Hurricane Recovery	XIVII
Flood Recovery	XX
Earthquake Recovery	XV
Tornado Recovery.....	XXIV
Wildfire Recovery.....	XXVI
Appendix.....	XXVII
Inventory	XXIX
Unique Supplies Form	XXIX
Post Recovery Review	XXX
Disaster Recovery Kit Checklist.....	XXXI
Critical Business Functions Checklist	XXXIIIIII
Critical Business Functions Form:.....	XXXV
Vendor Assessment Form	XXXVIVI
Crisis Communications Checklist.....	XXXVIII
Media Communication Guidelines	XL
News Release Template.....	XLI
Sample Voicemail Template.....	XLIII
Addendums.....	XLII

Executive Summary

Objective/Purpose of the Preparedness Plan

The objective of the Preparedness Plan of SterlingRisk is to prepare personnel to successfully manage potential interruptions or disaster situations while also considering their personal safety during the recovery efforts.

SterlingRisk defines a Disaster as a sudden, unplanned event causing unacceptable damage or loss as defined or determined by a risk assessment; 1.) Any event that creates an inability on an organization's part to provide critical business functions for some predetermined period of time. 2.) In the business environment, any event that creates an inability on an organization's part to provide critical business functions for some predetermined period of time. 3.) The period when company management decides to divert from normal production responses and exercises its plan. Typically signifies the beginning of a move from a primary to an alternate location.

This plan will identify the necessary personnel and resources required for both disaster preparation and response. Furthermore, it will ensure that the proper steps will be carried out to permit the timely restoration of services and business functions. The plan should minimize decision-making during a disaster or interruption by listing all actions required to restore the ability to complete business processes.

The objective of the Preparedness Plan is to reduce the risk to the communications and data networks to an acceptable level by ensuring the restoration of critical business functions within the determined Recovery Time Objectives (RTOs). This plan will also minimize the risk of delay in setting up the recovery site through prior preparation.

This plan aims to ensure the continuation of services to customers as well as the protection of shareholder interests and the following of any regulatory requirements.

Note that this plan includes processes and procedures which are primarily intended for recovering the main Woodbury, NY headquarters in the event of an emergency. Since there is no critical I.T. related equipment or data stored in remote locations, the appropriate measures would need to be taken to ensure physical file recovery, and appropriate local vendors would be contacted to restore hardware & connectivity to the main office once applicable. Many of the remote site functions could be handled from employees working at home until the remote site has been fully restored or relocated. See Addendum F for specific remote site information.

Location of the Preparedness Plan

The most current revisions of this plan are to reside in the following locations at all times:

1. Online myAgility Account
2. Multiple Copies in the physical building
3. Multiple Copies off-site in safe deposit box, fire-proof safe, and Disaster Recovery Kit
4. Multiple Copies stored on network drives backed up in the Cloud

Definition of Crisis Management Team (CMT)

SterlingRisk Crisis Management Team will consist of executives as well as key role players (i.e. CEO, HR Director, I.T. Director, facilities manager, etc.) and the appropriate business owners of critical organizational functions who are responsible for recovery operations during a crisis. As a team they will:

- Decide whether or not the organization should declare an alert or a disaster.
- Provide direction and support to all employees and recovery support staff members.
- Monitor and coordinate the necessary recovery activities.
- Liaison with civil authorities, major customers, public relations, etc.

CMT Members, Roles & Contact Information

Name, Title, Specialist Roles	Contact Option	Contact Number
David Sterling, Chief Executive Officer	Work	516-773-8600
CMT Chairperson	Mobile	516-606-4000
	Home	516-942-5450
	Email Address	dsterling@sterlingrisk.com
	Alternate Email	
Donna Raab, Chief Talent Officer	Work	516-773-8645
CMT Administrator	Mobile	631-682-2768
Human Resources Specialist	Home	
Public Relations Specialist	Email Address	drab@sterlingrisk.com
	Alternate Email	
Michael Tampone, Chief Technology Officer	Work	516-773-8679
Technology Infrastructure & Operations Specialist	Mobile	516-521-5154
Relocation Specialist	Home	
	Email Address	mtampone@sterlingrisk.com
	Alternate Email	
Scott Chirls, Senior Information Officer	Work	516-719-8756
Technology Data & Reporting Specialist	Mobile	516-330-6602
	Home	

Name, Title, Specialist Roles	Contact Option	Contact Number
	Email Address	schirls@sterlingrisk.com
	Alternate Email	
Joanne Krush, Chief Financial Officer	Work	516-773-8605
Financial Specialist	Mobile	
	Home	
	Email Address	jkrush@sterlingrisk.com
	Alternate Email	
Sebally Queylin, Facilities Manager	Work	516-719-8779
Files and Records Specialist	Mobile	
Equipment & Furniture Specialist	Home	
	Email Address	squeylin@sterlingrisk.com
	Alternate Email	
Marci Waterman, Chief Operating Officer	Work	516-773-8604
Relocation Specialist	Mobile	917-658-6485
Claims Specialist	Home	
	Email Address	mwaterman@sterlingrisk.com
	Alternate Email	

CMT Member Individual Responsibilities

1. CEO/Chairperson:

The CEO/Emergency Operations Team Chairperson appointee is an officer or partner in the company who has key decision making powers relative to corporate financial decisions during a disaster emergency.

2. Administrator:

The Emergency Operations Team Administrator, under the direction of the CEO and other officers of the company, is the leader of the Emergency Operations Team. The Administrator will call together all members of the Emergency Operations Team and delegate specific assignments to individuals per the recovery event steps and the functions described below.

The Administrator must ensure that the Emergency Operations Team's emergency contact numbers are listed in the Plan, as well as secured off site. The Administrator is responsible for confirming successful completion of each recovery event assignment including "signing off" each event on the recovery event steps checklist. S/he must also confirm that all items listed for vaulting in the company "backup boxes" are accounted for prior to sealing and transporting.

If circumstances require, an Emergency Operations Team Assistant Administrator must be prepared to assume the duties of the Administrator.

3. Technology Infrastructure & Operations Specialist

The Technology Infrastructure & Operations Specialist is responsible for ensuring that all mission critical computer hardware, software & telecommunications equipment has been accurately documented in the plan. This includes hardware, software, telephone & fax lines, Internet circuits, and any other communications systems components. S/he will coordinate the replacement and installation of hardware, software & telecommunications equipment by vendor of choice, and will also take possession of any computer backup media and all other computer related materials. S/he will also be responsible for working with telecom and Internet providers to ensure rapid replacement of all necessary communications systems.

4. Technology Data & Reporting Specialist

The Technology Data & Reporting Specialist is responsible for ensuring that all critical systems data, customized applications & reports are documented in the Plan. S/he will be responsible for ensuring that all data is accurate and complete if restoration is required, and that all mission critical reports and custom applications are up and running as soon as possible after an emergency.

5. Financial Specialist

Throughout the recovery process, key financial decisions must be made based upon a thorough knowledge of the financial position of the company relative to cash reserves, accounts payable, accounts receivable and general cash flow. The CEO of the company

will make decisions based upon the financial information provided by the Financial Specialist.

6. Human Resources Specialist:

The Human Resources (HR) Specialist must be prepared to coordinate the activities of the entire work force. S/he is responsible for all post disaster communications with employees, and at the direction of the CEO, must be prepared to address issues such as; who is to report to work and where, who is to be laid off, who is to stand-by for instructions, etc. The HR Specialist is responsible for ensuring that all emergency contact phone numbers, addresses and any other information necessary to communicate with employees is documented and accessible during an emergency.

7. Public Relations Specialist:

The Public Relations Specialist under the direction of the CEO must compose communications for all appropriate parties including employees, clients, vendors and the media. The Plan contains sample post -disaster letters and media releases. S/he is responsible for editing these communications to reflect the circumstances of the disaster and to disseminate them to all appropriate parties.

8. Relocation Specialist

The Relocation Specialist will coordinate with your realtor of choice to begin steps to secure alternate temporary space. If temporary mobile office space is appropriate, the Relocation Specialist will work with your vendor of choice to arrange for delivery of trailers or other mobile facilities.

9. Files & Records Specialist

A vast amount of mission critical data may be contained in hard copy files that do not exist in an electronic media database. These files, which are often critical to disaster recovery and business resumption, must be salvaged from the disaster site if possible or re-created if lost. The Files Specialist must be familiarized with the hard copy files section of the Plan and be prepared to make decisions relative to restoration alternatives.

10. Equipment/Furniture Specialist

The Equipment/Furniture Specialist is responsible for confirming the accuracy of the "cold-site" and furniture requirements and office equipment documented in the plan. Photocopy machines, fax machines, postage meters and any other specialized equipment deemed critical for replacement at a "cold site" will be ordered for replacement by the Equipment Specialist. In addition, any printed materials such as company stationary, brochures, forms, bank checks, etc. are to be prepared by for vaulting in the company "backup boxes" as outlined in the Plan. S/he is also responsible for coordinating the ordering and delivery of replacement furniture from your vendor of choice and for contacting the appropriate delivery services such as USPS, Fed Ex, UPS, etc. to request holding deliveries or delivery to an alternate address.

11. Claims Specialist

Should there be a regional disaster, the Claims Specialist will be responsible for coordinating claims intake and processing. S/he will need to document all processes

necessary for proper claims handling & management, and make sure that this information is readily available in the event of an emergency.

Assumptions

This plan is predicated on the validity of the assumptions listed below:

The plan is written to cover a worst-case disaster situation. However the plan may also be activated in less than worst-case scenarios, with any potential interruption to business or imminent threat.

Things to keep in mind:

- Managers will keep all personnel affected by this plan aware of its current procedures and practices
- All personnel affected by this plan are responsible for understanding their role(s) under a disaster situation
- This plan will be continually maintained
- The recovery process documented in the plan should be tested annually
- All personnel must react quickly and effectively during the recovery process

Audience

Employees

Customers, upon request and following executed non-disclosure agreement (NDA)

Vendors, upon request and following executed NDA

Shareholders, Board of Directors, Executive Committee

Regulatory Positions/Auditors

Distribution

The plan is to be distributed within New Hire Packet, and redistributed upon Maintenance schedule, and with any changes.

Maintenance

The plan must be continually updated to reflect changes to resources (systems and personnel) as well as the business environment. Any significant changes to these resources would require that the appropriate section of the plan or Addendum be updated accordingly. Addendums containing such information should be reviewed/updated at least annually, regardless of whether or not any significant changes took place. The plan should be retested and personnel retrained on any changes. SterlingRisk will record any and all changes in the version control page. Refer to the Preparedness Plan Maintenance and Testing section for best practices regarding maintenance.

Risk Assessment

To plan for recovery you must understand what risks threaten your organization and employees.

This assessment checklist will guide SterlingRisk through identifying and rating these risks. You can then focus mitigation efforts on risks with higher *importance*, which is calculated by multiplying the *probability* (increasing 1 to 5) and *impact* (increasing 1 to 5) numbers. Use the blank rows to write in any other threats particular to your organization. SterlingRisk to consider risks to its supply chain in a separate checklist found in the appendix, so focus here on threats directly to your business and employees.

Risk	Importance ▼			Comments
	Probability	Impact		
Power outage: (consider whether your grid is a priority for utilities to restore quickly)	2	3	6	Server room is on generator but PCs would require generator recovery for prolonged outage.
	Impact	3		
Lost access to building: (i.e. due to pest infestation quarantine, crime scene, etc.)	1	3	3	Low probability. 80% of staff has remote access capabilities.
	Impact	3		
Critical equipment failure: (i.e. email server, key file server, UPS, etc.)	2	4	8	Email and other key applications (EPIC, Salesforce, etc) are currently in the cloud and mitigate the risk of significant business impact. Fileserver and other less critical applications would require data restoration and/or server reconstitution.
	Impact	4		
Phone/Internet outage: (i.e. cut cable, phone company power loss, phone server down, etc.)	3	3	9	Moderate probability. Automated failover to backup Internet circuit for both phone and Internet is setup. Phone system is also hosted, and mobile app allows for access even if primary service is down.
	Impact	3		
Fire: (i.e. wildfires, nearby building fires, chemical fires, etc.)	2	5	10	Low probability, however could be most serious overall threat if server room is damaged in fire. Could require offsite relocation with
	Impact	5		

				Agility or Continuity Centers.
Tornado and other high winds: (consider impact increased if building is not storm-proof)	Probability	1	4	Building likely to withstand even tornadic wind event with superficial damage. Secondary impacts would be larger.
	Impact	4		
Flood: (i.e. regional flooding from coast or rivers, pipe bursts/leaks, etc.)	Probability	1	3	Very low probability given the geography. We also occupy 2 nd & 3 rd floors.
	Impact	3		
Hurricane/seasonal storms: (consider winter storms represent similar risk for non-hurricane regions)	Probability	3	9	Significant probability. Damage to facility is unlikely, however secondary issues could cause need for backup Internet circuit, and/or power through Agility. Greater threat would be to regional damage, and service provider issues.
	Impact	3		
Earthquake: (consider supply chain effects, not just your own building)	Probability	1	4	Low probability given our location. Recovery efforts could vary greatly depending on strength and location of Quake.
	Impact	4		
Employee absenteeism: (consider those with unique skills or special needs for family)	Probability	4	4	Fact of life. Many employees have remote access if necessary. Most if not all employees have backups to their roles in the event of actual illness, etc.
	Impact	1		
Mass absenteeism: (i.e. pandemic, transportation strike/outage, etc.)	Probability	1	4	Remote access available for most employees in this scenario.
	Impact	4		
Explosion/Spill: (Keep in mind there is a heightened risk if near highway, railroad, airport, chemical plant)	Probability	1	4	Risk is low, but obviously impact could be high if it happened in close proximity.
	Impact	4		
Terrorism: (communications and transport likely to cause secondary challenges)	Probability	1	4	Response would vary greatly depending on nature of attack.
	Impact	4		
Denial of service, or other similar attack: (Could be on local facilities or hosted application(s)).	Probability	3	12	Attacks are becoming more common. If launched against one of our main vendors (Microsoft, Applied, Salesforce or multiple ISPs), there could be significant impact in our ability to do business. Because of the immense resources and failover options in place for these large vendors, while the impacts would be large,
	Impact	4		

				the duration would likely be short. A similar successful attack on our local Internet circuit could be mitigated by failover to backup until attack ceased or is stopped.
Ransomware, malicious or unintentional data destruction or similar attacks:	Probability	4	12	An attack that compromised local data may require restoration from backup. The actual impact would vary greatly based on the nature and volume of information affected.
	Impact	3		
Employee or customer theft of, or accidental loss of, company devices or protected data.	Probability	3	9	The risks associated with such actions are largely mitigated by various DLP monitoring, log monitoring, and MDM tools that have been deployed. Company owned mobile devices/laptops generally do not contain any sensitive information and are protected by encryption and passwords. However, in the event a motivated disgruntled employee were to intentionally exfiltrate data, or company owned equipment containing sensitive data was lost or stolen and fell into the wrong hands, then private company or client data could be used for a variety of purposes. Such actions could lead to financial losses and embarrassment for both the company and our clients. The actual impact would vary greatly based on the nature and volume of information affected.
	Impact	3		
Internal Unauthorized System Access or Acts of Sabotage	Probability	2	8	With most sensitive systems have sophisticated password and multifactor authentication, and system access is granted using the principal of
	Impact	4		

				<p>least privilege, if an employee were to gain access to systems they were not authorized to see/use, it could lead to potential adverse impacts, or unintentional/intentional destruction of data. For standard employees, much of this damage could be traced and/or reversed. However, if a privileged employee (such as an I.T. or development team member) were to intentionally try to sabotage a system, the damage could be much more substantial and harder to trace. Continued Log alert reviews by multiple people and periodic access control reviews would help to mitigate against these possibilities.</p>
Employee or Visitor Workplace Violence	Probability	1	4	<p>While workplace violence incidents are fairly uncommon and generally are not designed to target sensitive company data or systems, the potential physical damage or injury that could be inflicted upon employees, including high level employees, could pose a significant risk to the company. As such it is important to continue to educate employees on reporting any suspected potential incidents of violence, and how to properly respond should such an incident occur.</p>
	Impact	4		

Critical Business Functions

SterlingRisk has identified all the resources and personnel required to restore or reproduce this function *during a recovery*. These are the critical functions necessary to keep the business operating in the immediate aftermath of an emergency. All other business functions and staff would be brought online as the situation normalized.

Function	Importance	Max Downtime	Person/Team	Required Resources	Impacted Functions	Brief Process to Complete Function
Reporting Claims and providing claims reports to Sterling clients	High	2 Days	Claims manager/Claims Team	5 – 10 employees depending on volume. Supporting Hardware & Software & connectivity to allow connection to email, Agency Management system & Claims system	Claims Reporting	Claims are reported to us via electronic means (email/telephone) and need to be submitted to Insurance Company using appropriate forms. Manual process is possible using appropriate paper forms and facility with fax capabilities.
Servicing Clients & Marketing	High	2 Days	Various Team Leads (Large, Select, Personal, Benefits & Programs)	20 – 40 employees Supporting Hardware & Software & connectivity to allow connection to email, Agency Management system & supporting software.	Updating, Renewing, Canceling Policies & Coverages. Adds/deletes of locations, autos, etc Issuing Auto ID Cards & Certificates Providing Schedules of insurance New business marketing and binding	Clients contact us via electronic means (typically email/phone call) to make changes to policies or request information and/or assistance. Policies also may need to be renewed and cancelled.
Company Finances	High	2 Days	CFO and key members of Accounting Department	3 – 5 employees. Supporting Hardware & Software & connectivity to allow connection to email, Agency Management system & supporting software	Process Payroll, Deposits, Collections and pay insurance companies.	Payroll needs to be submitted to ADP. Check deposits need to be made with bank. Wires and other transfers need to be processed to pay Insurance Carriers.
Information Technology Functions.	High	2 Days	I.T. Director, Senior Information Officer & key I.T. Staff	4 employees. Supporting Hardware, Software & Connectivity to allow connection all systems	Hardware and software installs and restores.	Hardware & Software would need to be setup & Data restored.

					Troubleshooting employee issues Maintain infrastructure. Reporting	Employees would report issues on various systems. Management would need key reports to be generated .
Corporate Service & Facilities	Medium	3 Days	Facilities Manager & key Corporate service staff member.	2 employees. Supporting Hardware, Software and Connectivity to allow connection to email and supporting software.	Physical mail processing. Scanning and other document handling. Furniture and Environmental issues.	Mail would need to be picked up from and delivered to post office and processed. Incoming documents would need to be scanned and disseminated. Furniture would need to be setup and environmental conditions (AC/Heating, etc) would need to be taken care of.
Sales Activities	Medium	4-5 Days	CEO, President and key Sales and Inside Sales Staff	10 – 15 employees. Supporting Hardware, Software & connectivity to allow connection to email, Salesforce & supporting software	Sales calls. Sales meetings with prospects & clients.	Inside Sales team researches and contacts new prospects and coordinates with Sales team to attend prospect meetings. Existing client renewals meetings setup, etc.
Human Resources	Medium	4-5 Days	HR Director and key HR staff member.	2 employees. Supporting Hardware, Software and Connectivity to allow connection to email and supporting software.	Hires, Terminations and Recruitment. Personnel Issues.	Decisions on employee terminations and or hires would need to be made. Day to day personnel issues would need to be addressed.

**Alternate form with additional detail for each business function is available in the appendix.

** See attached Procedure Manuals (Addendum H) as well.

Communication Plan

SterlingRisk has developed a Crisis Communication Team (CCT) and the following communication strategy to ensure all critical entities of the organization are kept up-to-date and aware of the circumstances surrounding any business interruption.

SterlingRisk's primary communication decision maker/coordinator:

Donna Raab - Chief Talent Officer

The following individuals have been appointed back-up decision maker(s) and will complete the make-up of the CCT:

Michael Tampone – Chief Technology Officer

The CCT is responsible for establishing and maintaining communication among the following entities of SterlingRisk:

- ☒ Employees
- ☒ Clients/Customers
- ☒ Regulatory Agencies

The CCT will determine and document when to activate an emergency communication plan, using the following criteria:

- ☒ Duration of outage/interruption
- ☒ Severity of interruption
- ☒ Percentage/Number of employees, departments impacted
- ☒ Prolonged loss of contact with clients or vendors

SterlingRisk has developed the following communication tools for reaching employees, customers, and/or critical suppliers:

- ☒ One Call Now alert messaging system (Phone/Voice, Text & Email)
- ☒ Dial in voicemail box
- ☒ Applied CSR24 800 number backup service
- ☒ Agility Alert Notification System
- ☒ Website notification banners

SterlingRisk will continue to educate employees about the communications plan by:

- ☒ Documenting the crisis communication plan in hardcopy and electronic formats (including myAgility)
- ☒ Training current and new employees
- ☒ Reminding employees about emergency communications
- ☒ Testing these communication plans regularly.

Phone Recovery Template

(Zoom is provider for all Woodbury NY Local & Toll Free Numbers)

Phone Number	Forwarded To*	Associated Email Box	Instructions	Description
516-487-0300			Can forward to 866-430-5694 (CSR24 Call center) until main number can be re-established.	Main Number
516-487-0372	888-870-8496	mainfax@sterlingrisk.com	Can leave as is as long as email is accessible. Otherwise can forward to temporary or new main fax.	Main Fax
DID Ranges 516-301-3100 to 3199 516-719-8720 to 8819 516-773-8600 to 8719 516-417-5100 to 5299			Can forward to 866-430-5694 (CSR24 Call center) until local extensions can be re-established.	Internal DID extensions
516-622-1097	888-455-7421	request@sterlingrisk.com	Can leave as is as long as email is accessible. Otherwise can forward new fax.	Quest Fax Line1
516-719-8781	888-455-7421	request@sterlingrisk.com	Can leave as is as long as email is accessible. Otherwise can forward new fax.	Quest Fax Line2
516-487-6035	888-310-0739	claimsfax@sterlingrisk.com	Can leave as is as long as email is accessible. Otherwise can forward new fax.	Claims Fax Line
516-487-0498	866-380-4485	essentialspfax@sterlingrisk.com	Can leave as is as long as email is accessible. Otherwise can forward new fax.	Essential Services Fax
516-719-8798	866-620-4819	plfax@sterlingrisk.com	Can leave as is as long as email is accessible.	Personal Lines Fax

			Otherwise can forward new fax.	
516-719-8796				
516-719-8730				Robert Larocca Fax
516-719-8733				Accounting Fax
516-773-8710				Marketing/SBus (Toshiba)
516-487-7803	888-517-0433	groupfax@sterlingrisk.com	Can leave as is as long as email is accessible. Otherwise can forward new fax.	Group Benefits Fax
516-773-8635				David Sterling Fax
516-622-1095				Brad Dubler Fax
516-622-1098				MusicPro Fax
516-773-8659				Sales Fax (Toshiba)
516-719-8808				President Conf Line
516-719-8797				Mailroom Fax (Toshiba)

516-719-8806	888-870-8496	mainfax@sterlingrisk.com	Can leave as is as long as email is accessible. Otherwise can forward new fax.	Old Sales (FW to Main)
516-622-1093				Info Tech Fax
516-719-8726	(800-525-9072 may be associated with this line)			Programs (Toshiba)
516-622-1092				Deb's Fax (No Answer)
	888-867-9407	mtampone@sterlingrisk.com	Can leave as is as long as email is accessible. Otherwise can forward new fax.	Mike Tampone Fax
	888-529-0538	tbrown@sterlingrisk.com	Can leave as is as long as email is accessible. Otherwise can forward new fax.	TBrown Fax
	888-467-5407	humanresources@sterlingrisk.com	Can leave as is as long as email is accessible. Otherwise can forward new fax.	HR Fax
	866-260-7578	plfax2@sterlingrisk.com	Can leave as is as long as email is accessible. Otherwise can forward new fax.	WhitePLains Personal Lines Fax

Employees Contact List (Addendum A1 & A2 or on OneCallNow or myAgility)

Vendors Contact List (Addendum B)

Evacuation Plan (See Addendum G)

SterlingRisk will use the following procedures to create an Evacuation Plan:

1. List of major fire hazards associated with the normal use and occupancy of the building.
2. Identification and assignment of personnel responsible for maintenance, housekeeping and controlling hazard sources.
3. Ensure awareness of the procedure for reporting a fire or other emergency.
4. Clearly mark nearest exits in office.
5. Create building/office layout and map nearest exits.
6. Post the evacuation plan and building layout in highly visible locations. Floor plans to include the locations of the following: exits, primary evacuation routes, secondary evacuation routes, areas of refuge, manual fire alarm boxes, portable fire extinguishers and fire alarm control.
7. Delegate an evacuation point person and an alternate evacuation point person to contact emergency officials, conduct a personnel head-count, update the evacuation plan, communicate the plan to personnel, etc.
8. Determine and clearly communicate assembly points for the employees in the event of an evacuation.
9. Practice the evacuation plan regularly.

SterlingRisk will use the following procedures to create an Emergency Shelter Plan

1. Delegate a shelter point person and alternate shelter point person to conduct head counts, contact emergency officials, stock emergency supplies, update emergency shelter plan and communicate the plan to the employees, etc.
2. Develop and document procedures of employees who must remain to operate critical equipment before evacuating.
3. Determine the location of the Emergency Shelter and assemble maps for employees.
4. Prepare personalized emergency supplies for employees (as needed) including; medical supplies, emergency medications, food/drink, etc.
5. Prepare general emergency supplies, including first aid kits, flash lights, batteries, radio, etc.
6. Practice the emergency shelter plan on a regular basis.

Preparedness Plan Maintenance, Training, and Testing

SterlingRisk recognizes that a Preparedness Plan is never truly finished, and there are three facets to the ongoing Planning Program.

- 1) The consistent upkeep and maintenance of this plan will ensure its accuracy and validity at time of disaster.
- 2) Regular training of new and current employees makes the written plan translate into a successful physical recovery.
- 3) Exercising and testing the various Plan elements will allow us to make corrections and improvements to the Plan as well as practicing its implementation in a controlled environment.

Maintenance of Plan

The SterlingRisk Plan will be kept up-to-date and accurate both proactively and reactively. Firstly, any relevant Human Resources, Technology, and Workflow changes in our production environment will be reflected in immediate and appropriate updates to our recovery Plan. The identification of these changes is the responsibility of the Director of the Department or Business Unit making the change, and the update to the recovery Plan is to be made by the Disaster Recovery Planning Team. Any update must then be logged in the Version Control section, and a new version assigned.

On a regular basis the SterlingRisk Crisis Management Team will meet for a Plan read-through. The goal of this meeting is to identify corrections or changes to the wording and content of the Plan required by employee or other resource changes since the last read-through. For example, the addition of a critical server or the replacement of a key recovery team member must be reflected in an update to the recovery Plan. Again, any update must then be logged in the Version Control section, and a new version assigned.

Training Employees

SterlingRisk recognizes that our written Plan is only as good as the people implementing it. With that in mind, we will have regularly scheduled training to orient new employees and remind existing employees regarding their part in a disaster recovery.

Mandatory participants include all full-time employees who have not attended a previous training session and all employees who are listed as having one or more responsibilities at time of recovery. Training will be scheduled and moderated by the Disaster Recovery Planning Team and will consist of an overview of the company recovery planning program and expectations of employees if a disaster is declared. This includes setting expectations of communication during a recovery so employees know how they will be reached and how to reach the management team.

Testing/Exercising of Plan

SterlingRisk recognizes that our plan should be tested at certain intervals to verify it's effectiveness, and to learn ways to improve it. Since we use Agility Recovery as our recovery partner, they offer a complete and robust testing program that we will utilize for regular exercises of the SterlingRisk recovery Plan.

This experience begins with a call or email to Agility Client Services (877-364-9393 clientservices@agilityrecovery.com). An Agility Test Coordinator is assigned and will arrange conference calls to discuss and handle all logistics including test objectives, equipment transportation, configuration requirements, and meal, hotel and transportation recommendations as needed. All of this information will be documented in an Agility-provided Testing Roadmap, of which a sample can be found [here](#). In addition, an Agility Technical Specialist and Network/Phone Specialist will be on hand to guide all technical planning ahead of the exercise and troubleshoot any technical issues during the exercise. Upon conclusion of each test, SterlingRisk will review (internally and with the Agility test team) all test notes to understand lessons learned and then make appropriate updates to the Plan itself.

The annual budget includes travel expenses plus the Agility test fee of \$1,500 for an Agility-site test or \$500 plus shipping for a technology test at our site. One or more appropriate test types will be selected from the examples below based on what portion(s) of the SterlingRisk Plan are deemed most in need of practice and validation.

Suggestions for Tests/Drills

- **Evacuation-** The first priority of this recovery Plan is safeguarding the well-being of SterlingRisk's employees. An emergency evacuation drill practices the safe and orderly evacuation of our building by all employees to a secure area away from the threat.
 - This evacuation drill will be built around a relevant scenario (office fire, tornado, local chemical spill, bomb or terrorist threat, etc.) but the goals and the steps followed are the same, regardless.
 - This drill can be performed as a planned, partially planned (only team leaders are fore-warned), or surprise event to test the speed and accuracy with which employees react to the perceived threat.
 - If the drill involves a simulated threat, such as a fire alarm being activated, local authorities (police and fire) should be fore-warned to avoid any confusion with false alarms from the activated system or employees.
 - Drills will be coordinated with other building occupants to simulate the traffic flows in a true evacuation.
 - Each department or team leader is responsible for his or her employees. This includes being aware of who is or is not present in the office at the time of the drill.

- Each department or team leader is responsible for notifying the Disaster Recovery Planning Team of any employee who temporarily or permanently needs special arrangements, such as a handicap-accessible exit.
 - The Disaster Recovery Planning Team is to time the evacuation and compare the result to the pre-determined goal time. The drill may be repeated more frequently if satisfactory results are not being achieved each time.
- **Tabletop-** A tabletop exercise is focused on applying SterlingRisk's Plan to a specific scenario and talking through each step. This is an effective way to identify any gaps in our Plan and to verify that key employees understand their roles and responsibilities in a recovery. This is a low-cost or no-cost way to test but is not a "functional test" as it does not require planned actions to be performed (like restoring a server or calling all employees). We have determined that a tabletop test should be performed at least once per year, in addition to coordination with Agility, but does not meet the requirement for full functional testing, as it is based on numerous assumptions that are not tested.
- **Emergency Communications-** Depending on the disaster situation there may be outages with standard means of communication such as work email and/or phones. Also, employees may disperse from the immediate area, making it difficult to contact employees to assist in the recovery and return to work in the recovery environment. A test of SterlingRisk's emergency communications plan using One Call Now or Agility's Alert Notification System on [myAgility](#) will accomplish a number of important elements: validate accuracy of employees' personal email and/or cell phone information, practice logistics of the Alert Notification tool, store sample alert messages for quick use in a disaster, perfect wording of alert messages, remind employees of how they will receive critical communications.
- **Power-** SterlingRisk can prepare for a potential power outage by completing Agility's Generator Requirements Document, making sure that they have all the information on file to provide us with a suitable generator when needed. A test of our power outage recovery plan can also be arranged through Agility, who will have a generator brought to our location and run to our electrician-installed power transfer switch. This can be done outside of office hours if needed. After the initial test for each site we should look to repeat the process every 3-5 years (or sooner if the electrical infrastructure is modified in any way) to validate our ability to recover from power loss.
- **Connectivity-** By testing SterlingRisk's voice/data communications over Agility's satellite link we can confirm connectivity with our key clients, key vendors, data center or core processor even if our normal lines are down. Agility can provide us with pre-engineered/custom solutions for our data connections and phone systems and test these either from our location (using a satellite dish shipped to us by Agility) or at one of their Test Facilities (both of which have permanent satellite installations). By configuring and testing these in advance we can save ourselves valuable time during a real disaster recovery

situation and have our communications with the outside world back up and running more quickly. After an initial connectivity test we should review our processes and communications needs on an ongoing basis, and re-run test exercises as needed.

- **Technology-** Agility will provide SterlingRisk with required IT infrastructure equipment with which to rebuild our key systems. In order to make a recovery as smooth as possible we should carry out practice runs for server restores and PC/workstation rebuilds using Agility's equipment. Establishing our ability to recover using Agility-provided hardware is vital to the ongoing integrity of our plan and, as such, we should look to test the recovery of our systems either by having Agility ship equipment to us, or by travelling to one of their Test Facilities (which would also enable us to simultaneously conduct a connectivity test if deemed appropriate). After initial testing we should conduct further exercises on an annual basis or more frequently as our equipment requirements or recovery processes change (including back-up solution, equipment upgrades, virtualization implementation, etc.).
- **Space-** SterlingRisk has the option to conduct a comprehensive recovery exercise with all Agility-provided elements, combining power, connectivity, technology and space in a single simulated recovery event. The recovery space can either be the standard mobile recovery unit or the brick-and-mortar retail space option available through Agility. This will provide the ultimate practice run for a disaster scenario by placing our employees and recovery assets in a fully realistic recovery environment. Due to the advanced complexity and cost, we do not plan to perform an exercise of this scope more than once every five years, but it is our goal to periodically exercise our Plan in this comprehensive manner in order to realize the benefits of testing in a realistic recovery environment.
- **Supply Chain-** SterlingRisk recognizes that the effectiveness of our recovery may hinge upon functions outside of our direct control. As our testing program matures we hope to include key vendors and clients in our exercises to increase the realism and learn how we will communicate and work together for mutual recovery of our supply chain network. We have determined that the most effective way to begin this aspect of our testing program is by practicing our communication with Agility, as our business continuity vendor will be the first and most directly important vendor we work with in a disaster recovery.

As part of our testing we may schedule a 'Mock Declare' with Agility by notifying our contact at clientservices@agilityrecovery.com of the day (time need not be determined) that we plan to call. On the specified day we will follow the steps to initiate a recovery with the goal of practicing and understanding how we will work with an Agility contact in a true disaster. **The caller must identify during the initial call that this is a mock declare.** Otherwise, costs could be incurred recovery resources being deployed due to a misinterpretation of this exercise.

Additional Testing and Training Resources

- [Agilitytest.info](#) – Agility has provided additional testing information including third-party articles, recorded Webinars, and suggestions on how to test most effectively with Agility.
- [www2.agilityrecovery.com/assets/DSI/testmap10.pdf](#) – Sample Testing Roadmap is an example of the custom documentation Agility will provide for each test exercise we complete with them. These will be filed for reference.
- [myAgility](#) – SterlingRisk’s private portal for Business Continuity Planning includes informative materials on all aspects of our Agility membership. For security reasons, we will print information from here for employees upon request rather than providing login information to all employees.
- [agilityrecovery.com/about/events](#) – Upcoming educational Webinars and other events.
- [preparemybusiness.com](#) – Recorded educational Webinars on various continuity planning topics.
- Social Media- [Facebook](#), Twitter, Blog

Training and Testing Log

The log will track all changes made to this Plan as well as any training and testing activities completed. This will allow SterlingRisk to track compliance with the expected frequency of each activity outlined in the preceding sections. Also, we can note when particular changes to the plan are implemented, and track version control. Each change made to this Plan will be logged with a new Version number, prompting the new Version to be distributed to all Plan storage locations.

Type	Description	Date	Version
Training	Example: All business units attended workshop on their roles. Next training tentatively scheduled for 11/15/2010	2/1/2010	1.1
Testing	Example: Data restoration and networking test at Agility's Atlanta test center. Also did a mock declare exercise with Agility. Updated plan, see version control	4/1/2010	1.2
Testing/Enactment	In March of 2020, the COVID 19 pandemic forced us to enact a portion of our BCP plan. A series of internal technical and administrative meetings were conducted to discuss the preparations and challenges that would be encountered, most notably was ensuring that all users would have uninterrupted remote access to all necessary systems, and making sure that internal infrastructure was re-enforced/tested/upgraded as needed. As the year progressed, we held routine meetings to assess and address our posture, and adjust accordingly, and sent out communications as necessary.	4/1/2020	1.3
Continued partial enactment	2021 continued to require at least partial enactment of our Mass Absenteeism due to COVID. As the hybrid / remote model evolved, we continued to evolve our systems, processes and testing.	11/22/2021	1.3

Recovery Procedures/Incident Response

Recovery ProceduresII

Power Recovery Overview III

 Power Recovery Process IV

Space Recovery Overview VI

 Space Recovery Process VIII

Technology Recovery Overview IX

 Technology Recovery Process X

Connectivity Recovery Overview XI

 Telecom Recovery ProcessXII

Communications Overview XIII

 Alert Notification Procedures XIV

Recovery Checklists..... XIV

 Winter Weather RecoveryXXV

 Hurricane RecoveryXVII

 Flood Recovery XXIV

 Earthquake Recovery XXVI

 Tornado Recovery XXIVIV

 Wildfire Recovery XXVIVI

Recovery Procedures

SterlingRisk has contracted with Agility Recovery to help us recover in the event of an interruption. We have access to power, space, technology, and connectivity as well as expert advice and coaching for any type of interruption. The following section will outline the service offerings available with Agility as well as step by step recovery procedures to follow after an interruption.

SterlingRisk will follow the Disaster Declare Procedure outlined below to formally notify Agility of a disaster.

CALL AGILITY - 877-364-9393

If after 5 p.m. ET, you may either dial “1” to contact an Agility team member or call an alternative hotline number (888-242-3740 or 866-894-3336).

SPECIFY

(Alert or Declaration)

- *Alert* – notifies Agility of a potential interruption (i.e. a server failure or severe storm is predicted).

By engaging Agility in advance, both parties may strategize and prepare for the coming event. The alert stage is not a required part of declaring a disaster but allows for the possibility of gaining valuable advice, guidance, costs and timeframes from Agility in preparation for recovery.

- *Declaration* – Initiates the recovery process for any or all of the recovery elements for alternative power, workspace, technology, and connectivity. SterlingRisk will be provided with a detailed cost estimate and recovery timeline for approval, prior to recovery mobilization.

AUTHORIZE

Agility will provide guidance, suggested strategies, present costs and timelines to better inform SterlingRisk of all of our potential recovery options. No costs will be incurred until SterlingRisk has approved all estimated costs associated with recovery. This approval will be made by voice verification by an authorized employee of SterlingRisk on a recorded line by Agility at time of declaration. Members of SterlingRisk that are authorized to Declare with Agility are listed in the ‘Contacts Section’ of our myAgility Recovery Profile (See Adendum).

Power Recovery Overview

Agility Recovery Provides SterlingRisk with the ability to recover from a power loss to our building with the use of a portable generator, power distribution unit as well as the required cabling. Generators are available in a variety of sizes and are located in multiple staging yards within our state and region.

SterlingRisk's generator requirements are listed in the 'Power Section' of our myAgility Recovery Profile.

Placement

The generator is to be placed on the southwest corner of the building's parking lot, where it will be best secured and accessible for refueling. We have permission from our landlord to park a generator here for emergency usage.

Connection Options

- **Transfer Switch** – allowing easy transfer from utility power to generator based power through an installed switch on the building.
- **Power Distribution Unit & Generator** – bypasses the electrical panel and provides power directly to the source of outage (server or telephone room, workstations).
- **Hardwiring** – requires a certified electrician to tie the generator directly into the electrical system. Also requires uninstall by electrician after utility power is restored.

SterlingRisk Responsibility

- Security (suggested measures)
 - Block the front of the generator by putting an obstacle such as a vehicle in front to prevent removal of the unit.
 - Install wheel locks on the generator trailer.
 - Run a chain through the tires of the generator trailer and lock them.
 - Remove the bolt and nut securing the hitch of the trailer mounted generator to prevent removal.

Things to keep in mind with power recovery are:

- Generator costs include a flat weekly rental plus transportation, fuel and electrician fees (if applicable).
- Once the generator is ordered from Agility, SterlingRisk is responsible for a minimum of the first week rental and transport even if power is restored in transit.
- Agility can provide assistance with both sourcing fuel as well as an electrician for our recovery.
- SterlingRisk is responsible for the equipment while in our possession including the security of the unit.
- Agility can set up a refueling schedule for the recovery.
- If using our own fuel vendor, we will check fuel gages frequently to ensure sufficient fuel levels at all times.

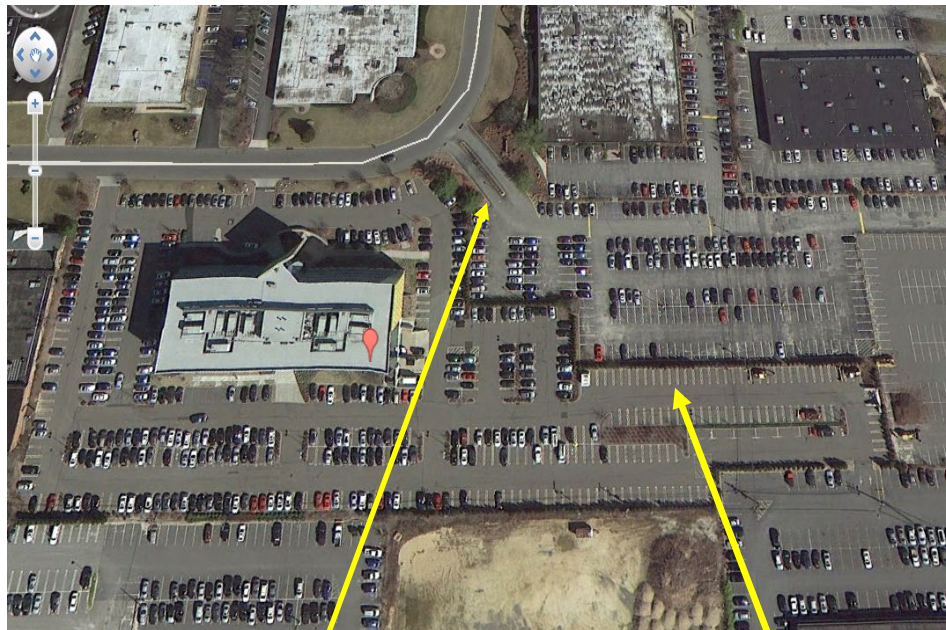
- Refuel generator upon completion and stand down of recovery. Fuel charges will apply for generators returned empty.
- Disconnect the unit and assemble all components for pick up, the driver is only responsible for loading the components and transportation. If using an Agility electrician, Agility will arrange for disconnect.

Power Recovery Process

Our building or a portion of the office space has lost power. Put Recovery Plan in action:

1. Leave the office and assemble at one of our designated assembly areas (illustrated below) to account for all employees.

←North DESIGNATED ASSEMBLY AREAS



SECONDARY ASSEMBLY AREA

PRIMARY ASSEMBLY AREA

2. Call Power Company and request timeframe for power to be restored and the cause of power loss (Ensure phone number and account number is programmed into Crisis Management Teams cell phones for quick retrieval).
3. **Contact Agility at 877-364-9393 and place on Alert.**
4. If outage estimates are longer than the durations below we will follow the following procedure:
 - 1-2 hours:
 - Wait out the outage
 - Server room is on building generator so servers and VOIP infrastructure (phones are all POE) should not be affected.
 - 2-4 hours:

- Update website to alert customers of outage and list alternate means to contact us if it becomes necessary to close office.
 - Set main number to Emergency Auto Attendant, and alert CSR24 to situation.
 - Use mobile devices (Email and Zoom VOM App) to respond to customer requests, and update email Out of Office Agents to alert customers of the issue and provide alternate ways to get in touch.
- Next Day:
 - Can continue to use mobile Zoom App or softphones, also can utilize Agility's phone redirection to voicemail option for DIDs if needed.
 - Setup key employees with Remote Access to Terminal Servers (Since server room is on building generator).
- 2+ days:
 - Request a generator from Agility and make necessary arrangements with electricians and building management corp to have proper connections made for hookup to our suites.

Space Recovery Overview

Agility Recovery provides SterlingRisk with the ability to recover when access to our building/office is not permitted. They can provide mobile, retail, move in ready, and commercial office space in a variety of locations and sizes. Agility will provide all the necessary technology, desks, chairs, generator and satellite access we need to get back-up-and-running at the recovery site.

SterlingRisk's space requirements are listed in the 'Space Section' of our myAgility Recovery Profile.

Space Options

- **Mobile Office** – allowing office space to be brought to our existing office or designated alternate recovery site within our community.
- **Move in Ready Office** – fully furnished existing space with desks, chairs, waiting area, conference room tables and break room facilities with technology and support supplied by Agility.
- **Retail Office** – Allows for walk up access for customers to conduct business face to face. Located alongside other businesses within an in-line space shopping center. Agility to provide tables, chairs, technology, connectivity and power if needed.
- **Mobile Office Parking Space** – shopping mall parking lot space availability in designated areas.

SterlingRisk Responsibility

- Mobile Site Security (suggested measures)
 - Use monitoring capabilities of existing security provider.
 - Agility can provide door and window bars on the mobile unit.
 - Arrange for physical security (i.e. security guard, police officer).
 - Construct temporary fencing.
 - Arrange for exterior lighting.
- Mobile Space Requirements and Site Suitability
 - Approximately 8 parking spaces for single-wide mobile office.
 - Approximately 30 parking spaces (15 spaces by 2 rows) for double-wide mobile office.
 - 14 feet of clearance at the access to the recovery site.
 - Recovery site is accessible 24 hours a day, 7 days a week.
 - Gravel, concrete/ asphalt is the preferred surface material.
 - Recovery site should be flat and mostly free of site obstructions (fire hydrants, trees, buildings, parking curbs, etc.).
- Retail Office Utilities Setup
 - Agility will provide contact information for the landlord who SterlingRisk will work with to coordinate utilities such as power, water/sewer, security, etc.

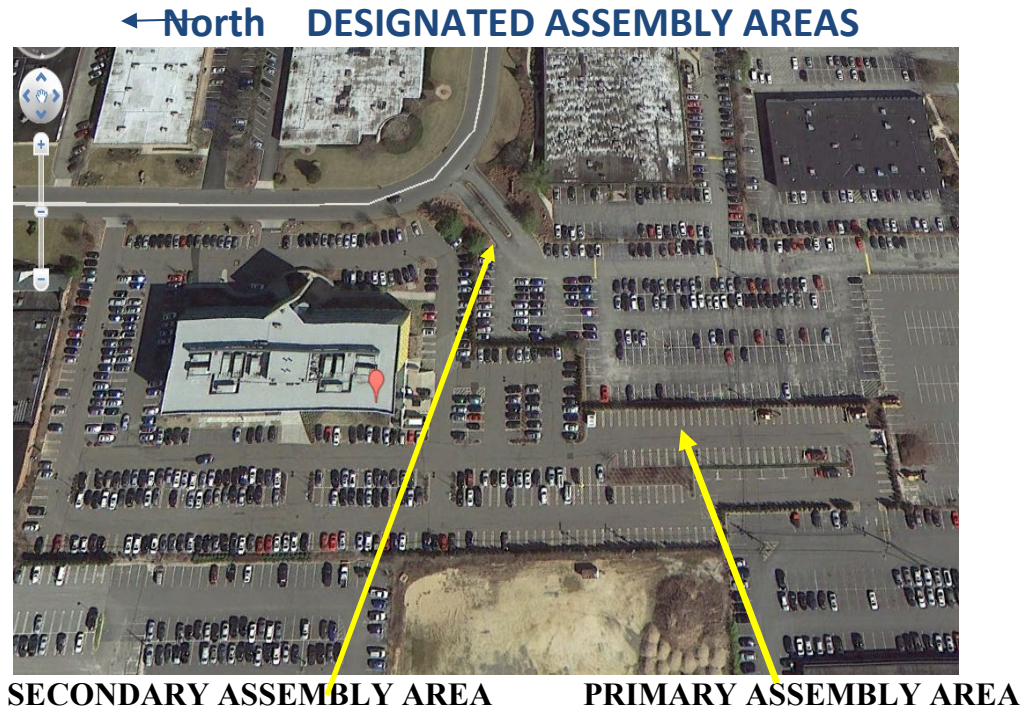
Things to keep in mind with space recovery are:

- Employee transportation and parking at the recovery site (carpooling).
- Employee and vendor communication about recovery location and/or status of recovery site.
- Communication with your clients about recovery location and/or status of recovery site (signage, company Web Site, emails, etc.).
- Mail and delivery services continuity.
- Restroom options (stand-alone portable solution(s), mobile office restroom, or local building).

Space Recovery Process

We have lost access to all or a portion of our office space. Put Recovery Plan in action:

1. Leave the office and assemble at one of our designated assembly areas (illustrated below) to account for all employees.



2. Complete damage assessment of the building to determine location of recovery (in our existing building or with Agility) as well as potential length of recovery.
3. Contact Agility at 877-364-9393 and place on Alert.
4. Follow the following procedure:
 - Determine roster for recovery site
 - Provide directions to recovery site for employees, vendors and clients
 - Contact vendors and update them with new address and modified work-flow process while in recovery
 - Train employees with new environment (close work-space condition, new equipment, etc.)
 - Execute a communication strategy with clients and the media (see Media Communications Guidelines in the appendix).

Technology Recovery Overview

Agility Recovery provides SterlingRisk with the ability to recover from a potential technology failure by providing us technology equipment. Below are the technology requirements for recovery.

SterlingRisk's technology needs are listed in the 'Computer Systems Section' of our myAgility Recovery Profile.

*Agility will provide equivalent or better technology as listed in the 'Computer Systems Section' of our myAgility Recovery Profile.

* Specific schedules or hardware addendums will supersede the equipment identified in myAgility.

*Agility PCs are pre-loaded with a Windows Operating System; however no additional software/applications or data is installed.

*Agility servers are not pre-loaded with an Operating System nor software/applications or data.

SterlingRisk Responsibility

- Restoring software/applications and/or data(options)
 - Contact third-party IT vendor
 - Restore with PC imaging
 - Restore with server imaging
 - Restore with virtual machines
 - Restore with electronic (online) backup
 - Restore with storage device (i.e. NAS, SAN, external hard drive)
 - Restore by connecting to an off-site data environment (i.e. datacenter)

Things to keep in mind with technology recovery are:

- Backup software/applications and data on a regular basis (hourly/daily).
- Store backups of software/applications and data offsite (i.e. another office, storage facility, bank vault).
- Write a procedure for restoring software/applications and data.
- Practice executing your procedure for restoring software/applications and data on Agility's equipment.
- Involve your IT vendor with writing a procedure for restoring software/applications and data as well as the testing of that procedure.
- Confirm the service level agreement with your IT vendor ensures they will be available to perform/assist your technology recovery whenever it is needed.
- Know all steps and/or elements involved with restoring software/applications and data (i.e. passwords, power cords, license keys, decrypting encrypted backups, etc.).
- Ensure your backups can be restored to dis-similar equipment.
- Have clearly defined roles and responsibilities around restoring software/applications and/or data for your IT vendor(s).

Technology Recovery Process

We have a potential or actual technology failure. Put Recovery Plan in action:

1. **Contact Agility at 877-364-9393 and place on Alert.**
2. SterlingRisk will follow the IT Recovery Plan below to restore our hardware, software and data.

Technology Recovery Plan Action Items:

- Asses extent of damage and or number of PCs, Servers, Switches, Phones, Printers, etc that need to be replaced (Use as much existing hardware as possible).
- Contact technology vendor and ascertain the time frame necessary to replace key pieces of hardware. If downtime is unacceptable, call Agility and request the appropriate recovery technology for use during this interim period.
- Alert off site backup vendors (see Addendum B) that recovery of data may be necessary, and have appropriate physical drives shipped out if necessary.
- Establish core network back-bone with new/rented/existing equipment (ie: Firewall, router, switches, printers and other basic networking infrastructure).
- Install required Server OS software on specified servers using Microsoft server install programs and SterlingRisk license keys (see Addendums C & D).
- Install necessary Server software and initiate data recovery with assistance of Offsite backup vendors. (Data Storage Corp requires separate PC or Server “Backup Station” to install the Asigra backup software. OnlineBackupVault requires the install of their Java based software on each machine requiring a restore).
- Active Directory Controller servers should be configured and recovered first, followed FileSharing server & Application servers. Other servers can be restored later on in the process.
- As core servers are being restored, master PC should be setup with all necessary OS, software & printer drivers. (refer to Addendums C & D).
- Once master PC is setup and configured to connect to network successfully, then replication should begin using Norton Ghost on USB drives to restore image to other PCs (
- can also utilize Agility PC cloning services).
- In tandem to the above, as data is restored, it should be spot checked for accuracy and completeness.
- Verify connectivity to all cloud based applications once Internet communication has been restored (Per Connectivity Recovery Process).

Connectivity Recovery Overview

Agility Recovery provides SterlingRisk with the ability to recover from a telephone and/or Internet outage by providing us access to a remote voicemail and/or satellite connectivity for Internet and telephones.

SterlingRisk's communication requirements are listed in the 'Communications Section' of our myAgility Recovery Profile.

Agility Connectivity Options:

- **Bandwidth-** 3Mbps to 10Mbps
- **Satellite Internet** – Provided
- **Public IP Address** –1
- **VPN Connectivity** – Available upon request (a one-time engineering cost will apply)
- **Voice Services-** Voice over IP (VOIP), Voicemail, Call hold, Call transfer, 3-way calling, Auto attendant, 5 DID numbers (Additional customized voice solutions available upon request)
- **Phone Redirection** – Recovery by remote voicemail which can be put in place very quickly and be managed by either calling into the voicemail or receiving an email with the voice message attached.

*Specific schedules or bandwidth addendums will supersede the equipment identified in the chart above. SterlingRisk will inquire about additional bandwidth needs if necessary.

SterlingRisk Responsibility

- Phone Redirection
 - At time of recovery, Agility will provide the phone number(s) (DIDs) for SterlingRisk to provide to their telecom provider.
 - SterlingRisk will work with their telecom provider to establish a call redirection plan (See Phone Recovery Template). (Should not be necessary as Zoom is cloud based, and VOD, VOM and VOIP Phones can be used).
- Internet Security (options)
 - Site-to-Site VPN (Virtual Private Network) – An Agility engineered solution prior to a recovery and/or test which is very efficient in high-latency environment such as a satellite network.
 - End-to-End VPN (Virtual Private Network) –VPN tunnel, which is hosted and managed by SterlingRisk at their recovery site.
 - Software VPN (Virtual Private Network) – PC software/applications to host individual connections to a hosted network (i.e. Citrix).
 - MPLS – connect into SterlingRisk's secure MPLS network via a VPN.
 - Firewall – Controls access into the local network after being installed at the recovery site.

Things to keep in mind:

- Faxing takes a considerable amount of bandwidth. Alternatives to traditional faxing such as eFax typically allow for better performance in recovery.
- Employee training for a recovery environment. Keep in mind, a recovery environment is typically a consolidated work place and you will need to plan for new aspects such as noise level and personal spacing.
- Agility provides a default phone hand-set, however you may consider bringing headsets to use during recovery.
- Agility will provide a phone guide for the phone hand-sets to assist with employee training on new equipment.
- Prioritize work tasks to ensure the most critical business operations will have the most bandwidth (Internet speed and phone volume) allocated for use.

Telecom Recovery Process

We have had our phones go down. Put Recovery Plan in action.

1. Contact the Telephone Company and understand cause/source of outage as well as timeframe for restoration. *Make sure you understand the process for redirection or forwarding your phone numbers to alternate numbers that Agility will provide for you (see template below).
2. **Contact Agility at 877-364-9393 and place on Alert.**
3. *If outage estimates are longer than the durations below we will follow the following procedure:
 - 1-2 hours:
 - Wait out the outage
 - Server room is on building generator so servers and VOIP infrastructure (phones are all POE) should not be affected.
 - 2-4 hours:
 - Update website to alert customers of outage and list alternate means to contact us if it becomes necessary to close office.
 - Set main number to Emergency Auto Attendant, and alert CSR24 to situation.
 - Use mobile devices (Email and Zoom VOM App) to respond to customer requests, and update email Out of Office Agents to alert customers of the issue and provide alternate ways to get in touch.
 - Next Day:
 - Can continue to use mobile Zoom App or softphones, also can utilize Agility's phone redirection to voicemail option for DIDs if needed.
 - Setup key employees with Remote Access to Terminal Servers (Since server room is on building generator).

- 2+ days (if generator fails):
 - Request a generator from Agility and make necessary arrangements with electricians and building management corp to have proper connections made for hookup to our suites.

Communications Overview

SterlingRisk utilizes the OneCallNow Emergency Alert system, which provides us with the ability to communicate with our employees and key contacts (such as vendors, suppliers, distributors, clients, etc.) over an online Alert Notification System. In addition, Agility Recovery provides us similar functionality as part of our myAgility account, should we have any issues with OneCallNow or need additional capabilities.

Things to keep in mind with communications during recovery are:

- Both OneCallNow and The Agility Alert Notification System require that you have all of your contacts loaded prior to using the communication tool.
- Determine communication strategies with your Crisis Management Team (CMT). Assign alternates for team leaders in the event they cannot be reached during a disaster.
- Have alternate communication plans (i.e. phone tree, 2 way radios, Website, Facebook, etc.) with the understanding that Internet access or cell networks, etc. may be unavailable during a disaster.
- Ensure your audience has a way to communicate back with the Crisis Management Team.
- Be aware of the best communication method (Website, phone call, etc.) to reach your intended audience and make sure your communication strategies are appropriate for reaching them.
- Teach, train, and continue to reinforce your communication strategies with your employees and key contacts.
- Conduct tests of your communications strategies to ensure your intended audience is receiving the message(s).

Alert Notification Procedures

Telephone service is not operational. Put Communication Plan in action for Alerting Employees, Vendors and Clients:

1. SterlingRisk's Crisis Management Team (CMT) Leader or alternate will sign into OneCallNow or myAgility account.

SterlingRisk's OneCallNow and myAgility Login information is contained in Addendum B:

2. Complete the fields for name, email, subject and message.
3. Select the recipients individually or by employee department and/or vendor type.
4. Select if you would like to send either an email, voice message, or text message or all of the above to the recipients.
5. Create and send the alert message.

Recovery Checklists

Below are checklists for undergoing various types of recovery scenerios. Agility is our trusted advisor through any interruption and your partner in preparedness. When faced with an interruption please contact Agility to quickly recover, by dialing 877.364.9393.

Winter Weather Recovery

Winter weather brings concerns about heat and maximizing its retention, frozen pipes, and access to your place of business.

The following checklist will help you identify the areas of your business that are most susceptible to winter hazards and to suggest ways to minimize damage. It is a good idea to develop a plan of action for your business and your staff to be ready for this type of interruption. Below you will find critical information and preparedness tools to assist in protecting your business and the most critical element of your business – your people.

✓	Before the Storm
	Check your insurance coverage for protection against winter hazards.
	Procedure for restoring electrical services on an item-by-item basis.
	Procedure for relocating salvageable and undamaged stock and supplies.
	Add the following supplies to your disaster supplies kit: rock salt (to melt ice on driveways), sand (to improve traction), and snow shovels (or other snow removal equipment).
	Determine your greatest risk potential: loss of heat, frozen pipes, and/or loss of access due to snow/ice.
	Identify who is responsible for keeping heating equipment in good working order: business owner or landlord.
	Identify who is responsible for snow/ice removal: business owner or landlord.
	Determine what equipment needs to be protected from freeze-up, i.e. computers, telecommunications, manufacturing equipment, etc.
	Are portable heaters or other emergency equipment needed?
	If snow and/or ice prohibit access to your business, are there alternative ways to enter your premises?
	Seal all openings with caulking and insulation where cold air can enter.
	Repair walls and roofs to prevent drafts; inspect roof drains for debris.
	Make sure storm windows are effective, if appropriate.
	Make sure heating and heat-producing process equipment is in good condition and operating efficiently.
	Arrange for snow removal from driveways, doorways, and roofs.
	Drain all idle pumps and compressors, making sure jackets are vented.
	Provide proper lubrication for cold weather operation (i.e., emergency generators, snow blowers).
	Test cold weather equipment.
	Clean and inspect boilers and firing mechanism/controls.
	Maintain automatic sprinkler protection in idle buildings; promptly handle sprinkler system impairments; notify local fire department.
	Monitor building temperature especially in hard-to-heat areas containing vulnerable equipment. Keep temperatures above 40°F.
	Mark hydrants near your business for ease in locating and clearing after a heavy storm.
✓	During the Storm

	Heaters, snow blowers, generators, and cold-weather equipment should be located where it is most likely to be used.
	Keep driveways, walkways, and doorways clear of snow and ice.
	Open water faucets slightly to let them drip in order to keep water flowing through the pipes that are vulnerable to freezing. Ice may still form, but the open faucet helps prevent the pipe from bursting by allowing relief for any built up pressure.
	Names and phone numbers of your heating contractor, plumber, fire department, insurance agent, and building owner should be easily accessible.
	Have someone assigned to check indoor temperatures should your place of business be vacant for long periods of time.
✓	Your People
	Ensure you have an emergency communication plan in place prior to the storm, evacuation, or threat.
	Have all employees, vendors, and client contact information on hand.
	Use the Alert Notification System on myAgility to keep all posted on status and next steps.
	During evacuation consider your phones lines- redirection to cell phones, answering service, Google Voice, or Agility lines could be critical.
	Following the storm, notify all critical people of next steps, based on damage.

Winter storms may range from a moderate snow in a short amount of time to a blizzard lasting for days. Some storms are regional and may affect several states, while others are more localized, depending upon geography and terrain. Common characteristics of winter storms are dangerously low temperatures, strong winds, ice, sleet, and freezing rain.

Know the Terms:

- **Winter Storm Watch**
Be on alert, a storm is likely.
- **Winter Storm Warning**
Take action, the storm is in or entering the area.
- **Blizzard Warning**
Snow and strong winds combined will produce blinding snow, near zero visibility, deep drifts, and life-threatening wind chill--seek refuge immediately!
- **Winter Weather Advisory**
Winter weather conditions are expected to cause significant inconveniences and may be hazardous, especially to motorists.
- **Frost/freeze warning**
Below freezing temperatures are expected and may cause damage to plants, crops, or fruit trees.

Hurricane Recovery

Hurricanes generate a series of threats to lives and property. The most obvious is the threat posed to buildings, equipment, and people by the high winds which characterize such storms.

This checklist will help you prepare for a hurricane's effect on your business, employees and community by highlighting activities you should undertake before, during, and following the event. When the National Oceanic and Atmospheric Administration's National Hurricane Center issues a watch or warning, use the advance warning to begin taking the following steps.

✓	Before the Storm
	Stay up-to-date on the storm's progress.
	Ensure you have an emergency communication plan in place prior to the storm, evacuation, or threat.
	Backup all data on servers and personal computers. If the backup site is within the area that may be affected by the storm, take backup tapes with you in the evacuation.
	Turn off all non-critical devices such as server monitors and workstations and other non-essential electrical equipment.
	Check the integrity of the uninterruptible power supply (UPS). Move the UPS to the highest level possible above the floor.
	Inspect and make emergency repairs to drains, gutters and flashing.
	Strap or anchor to the roof deck support assembly (e.g., the joists) all roof-mounted equipment such as HVAC units and exhaust vents.
	Call Agility to go on Alert.
	Protect/relocate vital records.
	Install windstorm shutters/plywood over windows and doors.
	Take the following steps so that items outdoors will not blow away or cause damage: <ul style="list-style-type: none"> ○ Remove all loose debris ○ Anchor or relocate all nonessential equipment to a safe indoor location ○ Secure storage of flammable liquid drums, or move them to a sheltered area (but never into main facility areas) ○ Anchor all portable buildings (e.g., trailers) to the ground ○ Secure large cranes and other heavy equipment ○ Make sure outdoor signs are properly braced
	Ensure that the employees who volunteered to stay on site have proper supplies and equipment (drinkable water, nonperishable food, medical, flashlights, walkie-talkies).
	Have cash on hand for post-windstorm needs, such as buying food and supplies, or paying employees and contractors.
	Ensure you know which employees are certified in CPR, EMT, etc.
	Repair and fill above-ground tanks with water.
	Fill fuel tanks of generators, fire pumps, and all company-owned vehicles.
	Remove as many goods as possible from the floor, or ship them out of the facility.

	Shut off gas to minimize fire loss.
	Disconnect the main electrical feeds to the facility, if possible, to prevent a potential fire caused by short-circuiting of damaged equipment.
✓	During the Storm
	Patrol the property continuously and watch for roof leaks, pipe breakage, fire or structural damage. During the height of a windstorm, personnel should remain in a place that has been identified as safe from wind and flood.
	Constantly monitor any equipment that must remain on line.
	During power failure, turn off electrical switches to prevent reactivation before necessary checks are completed.
✓	After the Storm
	Secure the site.
	Survey for damage.
	Call Agility and move forward from alert or stand down.
	Survey for safety hazards such as live wires, leaking gas or flammable liquids, poisonous gases, and damage to foundations or underground piping.
	Call in key personnel and notify contractors to start repairs. Make sure safety systems are fully implemented before work is allowed to begin. This means controlling smoking and other open flame sources. Require contractors to share responsibility for establishing fire-safe conditions before and during the job.
	Begin salvage as soon as possible to prevent further damage: <ul style="list-style-type: none"> ○ Cover broken windows and torn roof coverings immediately ○ Separate damaged goods, but beware of accumulating too much combustible debris inside a building
	Clean roof drains and remove debris from roof to prevent drainage problems.
✓	Your People
	Have all employees, vendors, client contact information on hand.
	Use the Alert Notification System on myAgility to keep all posted on status and next steps.
	During evacuation have a central point of contact for all employees, and ensure you know where your people are located.
	During evacuation consider your phones lines- redirection to cell phones, answering service, Google Voice, or Agility lines could be critical.
	Following the storm, notify all critical people of next steps, based on damage.

In flat areas, storm surges may rush many miles inland. Hurricanes often generate heavy rainfall, which can cause severe flooding over wide areas. Hurricanes also may spawn deadly tornadoes. Flooding and tornadoes may affect areas well inland. You should also prepare for these potential interruptions.

The National Weather Service rates hurricanes by their intensity, using a scale of one to five. The scale categorizes storms according to their sustained winds; the storm surges produced, and expected damage. Businesses located within areas of risk should have a hurricane preparedness plan. It is a good idea to develop a plan of action for your business and your staff to be ready for this type of interruption.

Know the Terms:

- **Tropical Depression**
An organized system of clouds and thunderstorms with a defined surface circulation and maximum sustained winds of 38 MPH (33 knots) or less. Sustained winds are defined as one-minute average wind measured at about 33 ft (10 meters) above the surface.
- **Tropical Storm**
An organized system of strong thunderstorms with a defined surface circulation and maximum sustained winds of 39–73 MPH (34–63 knots).
- **Hurricane**
An intense tropical weather system of strong thunderstorms with a well-defined surface circulation and maximum sustained winds of 74 MPH (64 knots) or higher.
- **Storm Surge**
A dome of water pushed onshore by hurricane and tropical storm winds. Storm surges can reach 25 feet high and be 50–1000 miles wide.
- **Storm Tide**
A combination of storm surge and the normal tide (i.e., a 15-foot storm surge combined with a 2-foot normal high tide over the mean sea level created a 17-foot storm tide).
- **Hurricane/Tropical Storm Watch**
Hurricane/tropical storm conditions are possible in the specified area, usually within 36 hours. Tune in to NOAA Weather Radio, commercial radio, or television for information.
- **Hurricane/Tropical Storm Warning**
Hurricane/tropical storm conditions are expected in the specified area, usually within 24 hours.
- **Short Term Watches and Warnings**
These warnings provide detailed information about specific hurricane threats, such as flash floods and tornadoes.

Flood Recovery

Floods are one of the most common and widespread of all disasters, and continue to grow in frequency and severity. Businesses are more likely to flood than burn down, so it is vital to prepare now.

The following checklist will help keep your business afloat even if the worst happens. Most businesses can save between 20% and 90% on the cost of stock and movable equipment by taking action to prepare in advance of flooding. The following resources and tools will help mitigate your risk and protect not only your business, but also the most critical element of your business – your people.

✓	Before the Flood
	Review Emergency Plan with team, and key employees
	Take all necessary steps to prevent the release of dangerous chemicals that might be stored on your property, Locate gas main and electrical shut-offs, Anchor all fuel tanks
	Postpone any receipt of goods- deliveries, couriers, etc.
	Contact insurance agent, discuss policy, etc.
	Establish emergency communication method (Alert Notification System, phone tree, etc.); identify meeting place and time for all key employees in Crisis Management Team; create voicemail for when evacuated, or out of office, etc.
	Update disaster recovery kits and begin crisis back-up procedures
	Maintain accurate inventory of product on site.
	Use plugs to prevent floodwater from backing up into sewer drains, or install flood vents/or flood proof barriers
	Stay tuned to local media & community messaging
	Contact Agility to go on Alert- this will enable you to exchange contact information, alternate information, and set up continuous communication times to discuss status
✓	During the Flood
	Life Safety is Paramount
	Begin next phase of your business continuity plan
	Send unneeded staff home
	Raise elevators to the 2 nd floor and turn off
	Stay tuned to local media- evacuate when required, safely
	Take cell phones and chargers with you & emergency kits
	Take all critical hardware with you, unplug electrical items, etc.
	Consider your business phones and redirection to cell phones, an answering service, Google Voice, or Agility lines
✓	After the Flood
	Listen for news reports to learn whether the community's water supply is safe to drink.
	Avoid floodwaters; water may be contaminated by oil, gasoline, or raw sewage. Water may also be electrically charged from underground or downed power lines.
	Be aware of areas where floodwaters have receded. Roads may have weakened and could collapse under the weight of a car.
	Clean and disinfect everything that got wet. Mud left from floodwater can contain sewage and chemicals.
	Implement DR plan, and monitor Local Authorities
	Contact employees via determined method of communication and discuss next steps.
	Contact your insurance agent
✓	Your People

	Ensure you have an emergency communication plan in place prior to the storm, evacuation, or threat
	Have all employees, vendors, client contact information on hand
	Use the Alert Notification System on myAgility to keep all posted on status and next steps.
	During evacuation have a central point of contact for all employees, and ensure you know where your people are located
	Following the flood, notify all critical people of next steps, based on damage

Helping to Mitigate your Risk for Flood Interruption:

Know the Terms:

- **Flood Watch**
Flooding is possible. Tune in to NOAA Weather Radio, commercial radio, or television for information.
- **Flash Flood Watch**
Flash flooding is possible. Be prepared to move to higher ground; listen to NOAA Weather Radio, commercial radio, or television for information.
- **Flood Warning**
Flooding is occurring or will occur soon; if advised to evacuate, do so immediately.
- **Flash Flood Warning**
A flash flood is occurring; seek higher ground on foot immediately.

Driving Flood Facts

The following are important points to remember when driving in flood conditions:

- Six inches of water will reach the bottom of most passenger cars causing loss of control and possible stalling.
- A foot of water will float many vehicles.
- Two feet of rushing water can carry away most vehicles including sport utility vehicles (SUVs) and pick-ups.

Earthquake Recovery

Most people would associate the risk of earthquakes with well-publicized and seismically active areas like California, parts of Washington State (especially in and around Yellowstone National Park) and some areas of Nevada and Utah. However the risk of earthquakes covers a much larger area of the United States and Canada.

The following checklist covers some basic points to consider in preparing for an earthquake which will help you recover more effectively in the aftermath. In the aftermath of an earthquake, these contingencies will prove vital activities ensuring that any damage to your business and resources are minimized.

✓	Before the Earthquake
	Be aware of your risk level. Add a map to your DR plan and make sure everyone is aware of the earthquake risk level in your specified region.
	Think about communications, since the chances are the phone company and possibly cell towers will be down. Your disaster recovery/response team will need to be in immediate contact with one another to ensure that your plan is activated and moving forward as quickly as possible. Think about two-way radios or text messages. The Alert Notification System on myAgility is also an invaluable communication resource.
	Develop a plan around communication, and deliver this to your team. Be sure to clearly identify each individual's roles and responsibility prior to the earthquake.
	Implement structural and non-structural hazard mitigation actions: bolting furniture to walls, ensure hardware and technology are secure, safety latches for cabinet doors, install fire sprinklers, use hook and loop fasteners to keep computers and other equipment from falling.
	Discuss coverage with your insurance provider. Understand your extra expense, and business interruption policies, before the interruption occurs.
	Contact your property owner or facilities manager and ask about having a laminate or plastic film placed on the inside of the windows to prevent glass shattering and endangering employees.
	Assemble and store emergency supply kit- for 3 days minimum (see checklist for emergency supply kit).
	Assemble building site maps and floor plans identifying exits, fire escapes, stairways, utility valves and shutoffs, fire extinguishers, hydrants, and standpipes, hazardous materials, and locked or restricted areas. Include these in your plan.
	Prepare your building for an extensive power outage and look at power options, particularly generator requirements. Contact Agility or your local electrician for assistance with this.
	Review your current data backup procedures and consider contracting with a datacenter or collocation facility that is in a different part of the country (one not prone to earthquakes, hurricanes or any other kind of aggressive natural events). Back up all your data to them on a daily (or at least every other day) basis, so that in the event you lose your networks and servers you can be back up and running and restoring your saved data to replacement equipment.
✓	During the Earthquake
	If you are indoors , duck or drop down to the floor. Take cover under a sturdy desk, table or other furniture. Hold on to it and be prepared to move with it. Hold the position until the ground stops shaking and it is safe to move. Stay clear of windows, fireplaces, woodstoves, and heavy furniture or appliances that may fall over. Stay inside to avoid being injured by falling glass or building parts. If you are in a crowded area, take cover where you are. Stay calm and encourage others to do likewise.
	If you are outside , get into the open, away from buildings and power lines.
	If you are driving , stop if it is safe, but stay inside your car. Stay away from bridges, overpasses and tunnels. Move your car as far out of the normal traffic pattern as possible. If possible, avoid stopping under trees, light posts, power lines, or signs.

	If you are in a mountainous area , or near unstable slopes or cliffs, be alert for falling rock and other debris that could be loosened by the earthquake.
	If you are at the beach , move quickly to higher ground or several hundred yards inland.
✓	After the Earthquake
	Employees should immediately check for injuries among fellow workers and render first aid. Seriously injured persons should not be moved unless they are in danger of further injury.
	Check for fire hazards, gas leaks, or damaged electrical wiring. Make sure main valves are turned off.
	Use flashlights (in emergency supply kit) vs. matches/lighters, due to potential gas leaks.
	Be prepared for aftershocks – these can come for several days after the main quake and can frequently topple already weakened structures.
	Consider relocation during recovery, depending upon damage to structure. Contact Agility for alternate space.
	Bring all vital records with you to your recovery site: data, employee lists, vendor lists, etc. Ensure you have access to your myAgility profile.
✓	Your People
	Ensure you have an emergency communication plan in place prior to the event, evacuation, or threat.
	Determine who is certified in CERT, CPR, etc. and what their responsibilities will be in the event of an earthquake.
	Use the Alert Notification System on myAgility, or internal employee hotline, to keep all employees posted on status and next steps.
	During evacuation have a central point of contact for all employees, and ensure you know where your people are located.
	During evacuation consider your phones lines- redirection to cell phones, answering service, Google Voice, or Agility lines could be critical.
	Following the earthquake, notify all critical people of next steps, based on damage.

Earthquakes are measured by the Richter magnitude scale. This is used to express the level of seismic energy released by the earthquake. The scale is theoretically limitless, although the highest magnitude so far recorded was 9.5 in 1960.

Intensity Scale	Description	Effects
less than 2	Micro	not felt
2-3	Very Minor	not felt but recorded
3-4	Minor	often felt, no damage
4-5	Light	shaking observed
5-6	Moderate	Some damage
6-7	Strong	damaging over a 100 mile area
7-8	Major	serious damage over wider area
greater than 8	Great	Serious damage over several hundred miles

Tornado Recovery

A tornado is arguably one of the most destructive types of storms imaginable. Unlike a hurricane or tropical storm, a tornado may develop almost without warning, appearing within minutes and leaving little time to react accordingly. Winds can get up to and exceed 200mph causing enormous damage in its path. Therefore, the importance of being prepared beforehand cannot be conveyed strongly enough.

The following is a checklist to prepare your business in the event of such an occurrence.

✓	Before the Tornado
	Have a weather alert radio in the office.
	Have a plan to provide emergency notification (warning system) to all employees, clients, visitors and customers in an emergency. The Alert Notification System in myAgility can be a valuable tool to assist in keeping communication lines open with employees.
	Put your crisis management plan in writing and give it to all employees.
	Conduct drills regularly to prepare employees for the real thing.
	When you establish your timeline for workplace preparation and closure, consider that employees will need to prepare their families and take care of personal matters as well. Allow enough time for them to execute their personal preparedness plans.
	Identify critical employees, and make sure they understand what is expected of them during a disaster. For example, you may need certain employees responsible for IT functions to work during a disaster to protect and reestablish your technology systems. If you need those employees to work remotely, make travel, hotel, and meal arrangements in advance, and ensure they know what equipment and support they will need to perform their duties.
	Develop a plan to allow your payroll, benefits, and HR functions to operate during a disaster, after a disaster, or during any period in which access to your workplace is restricted.
	If employees will be required to return to the workplace to assist in the recovery process before all services are restored , obtain an adequate supply of water, nonperishable food, first-aid supplies, generators, cleaning supplies, batteries, flashlights, and other necessities.
	Update your employee contact information regularly and at the beginning of any season during which natural disasters are more likely. For those in hurricane-prone areas, that means now.
	Look for the following danger signs: dark, often greenish sky, large hail, dark, low-lying clouds, and/or loud roar (similar to a freight train).
✓	During the Tornado
	If a Tornado Warning is issued or if threatening severe weather approaches, make sure employees:
	Move to an interior room or hallway on the lowest floor and, if possible, get under a heavy piece of furniture.
	Stay away from windows.
	Mobile homes/ work trailers, even if tied down, offer little protection from tornadoes and should be abandoned.
	Go to a pre-designated shelter area such as a safe room, basement, storm cellar, or the lowest building level. If there is no basement, go to the center of an interior room on the lowest level (closet, interior hallway) away from corners, windows, doors, and outside walls. Put as many walls as possible between you and the outside. Get under a sturdy table and use your arms to protect your head and neck. Do not open windows.
✓	After a Disaster
	Ensure the site is safe for re-entry. A third-party inspector may be necessary to achieve proper safety protocol.

	Contact your Agility Client Service Representative (1.866.364.9696). Agility will assist with ‘standing down’ from your alert or declare status and walk you through the necessary steps for restoring order.
	Communication following a disaster is critical. In advance, establish a communication plan that will work regardless of the nature of the disaster. For example, consider setting up a toll-free number or website, make sure they are operated out of areas that aren't disaster-prone and are located away from your workplace, and give employees instructions on when, how, and what to communicate through those methods following a disaster.
✓	Your People
	Ensure you have an emergency communication plan in place prior to the storm, evacuation, or threat.
	Have all employees, vendors, and client contact information on hand.
	Use the Alert Notification System on myAgility to keep all posted on status and next steps.
	During evacuation have a central point of contact for all employees, and ensure you know where your people are located.
	During evacuation consider your phones lines- redirection to cell phones, answering service, Google Voice, or Agility lines could be critical.
	Following the tornado, notify all critical people of next steps, based on damage.

Tornadoes are classified using the “Fujita Scale”, the intensities shown in the chart below:

Category	Wind Speed (MPH)	Intensity
F0	< 73	Gale
F1	73-112	Moderate
F2	113-157	Significant
F3	158-206	Severe
F4	207-260	Devastating
F5	261-318	Incredible

Wildfire Recovery

Impacts of a wildfire include direct property damage, cost of suppression and damage to personal property and natural resources. The severity of effects is directly related to the intensity and extent of the wildfire.

Below is a checklist of just some of the things to consider to prepare your business for such an event as well as to ensure the safety of the people within your organization.

✓	Before the Onset of a Wildfire
	Keep an adequate number of appropriate fire extinguishers in strategic locations (such as near loading docks and waste collection areas) and maintain them properly.
	Train key employees and their backups on how to use extinguishers correctly.
	Consider maintaining a water supply at your facility to control small fires until emergency personnel can arrive. You might install a water tank or install hoses and pumps to an existing swimming pool, pond, river or lake. Be sure the hoses are long enough and inspect them regularly.
	If your business is located in an area subject to freezing temperatures, be sure that water outlets and pumps are protected.
	Evaluate water levels in extreme hot and cold weather conditions.
	If your water pump uses electrical power, consider obtaining a gasoline- or diesel-powered pump or generator in case electricity is cut off during a fire. However, be aware of the risk of storing a large quantity of fuel. Use an appropriate storage facility that is protected against vehicle impacts and fire.
	Have appropriate tools, such as rakes, axes, saws, buckets and shovels, available to help control small fires while waiting for emergency personnel to arrive.
✓	During a Wildfire
	Go to a pre-designated shelter area such as a safe room, basement, storm cellar, or the lowest building level. If there is no basement, go to the center of an interior room on the lowest level (closet, interior hallway) away from corners, windows, doors, and outside walls. Put as many walls as possible between you and the outside. Get under a sturdy table and use your arms to protect your head and neck. Do not open windows. Evacuation orders will often be swift and accurate for affected areas. However, if unable to evacuate, stay inside and away from outside walls. Close doors, but leave them unlocked in case firefighters require quick access into your area.
	Turn on battery operated radio to get latest emergency information
	If your office roof is accessible by ladder, prop it against the building so you and firefighters have access to the roof.
	Mark your position clearly with anything that may signal rescue workers to your presence inside the building. This could be articles of clothing or bright colored material attached to the outside of your location.
	Close windows, vents, doors, blinds, etc. Shut off gas meters, pilot lights and propane tanks. Turn on all lights in the building to increase visibility in heavy smoke.
✓	After a Wildfire
	Immediately check the roof, put out any fires, sparks or embers (if accessible).
	Contact your Agility Client Services Representative for direction on 'standing down' from an alert or declare status.
	If there is no power, check to make sure the main breaker is on. Fires may cause breakers to trip. If the breakers are on and power is still not available, contact the utility company.
	ALWAYS contact 911 if any danger is perceived upon re-entry and contact local experts before finally moving back in.
✓	Your People

	Train your employees in general fire safety, especially for tasks with a high fire risk, such as welding and cutting, fueling vehicles, working with flammable liquids, etc.
	Teach employees about the importance of good housekeeping and grounds maintenance in preventing and controlling fires.
	Have an adequate number of appropriate fire extinguishers and maintain them properly.
	Train key employees in when and how to use fire extinguishers.
	Consider when and how to evacuate employees if a wildfire threatens.
	Establish an evacuation plan and keep it up to date.
	Hold evacuation drills regularly so all employees will know who is in charge and so that they become familiar with evacuation routes and routines.
	Make sure all employees can get out of the building, find shelter and communicate with a responsible person.
	Plan primary and secondary exits from your buildings. Consider how employees will escape if doors or windows are blocked by an exterior fire.
	Plan two evacuation routes out of your neighborhood. Consider how employees will evacuate on foot if roads are closed or impossible to use, such as if they are blocked by emergency personnel.
	Remember that ponds, lakes, rivers and landscaping or swimming pools can serve as safety zones.
	Keep appropriate emergency supplies on hand, including flashlights, battery-powered portable radio, extra batteries, first-aid kit, manual can opener, non-perishable foods and bottled water. If designated employees will be working to protect the property, have appropriate clothing available, such as work boots and gloves, personal protective equipment and sturdy work clothes.
	Teach employees about wildfire risks and preparedness. Provide information to help employees protect their homes, too.
	If you are located in a wildfire area, consider advising employees to keep personal disaster supplies and copies of important documents at work in case they need to evacuate from work without being able to get home.

A wildfire, or forest fire, is an uncontrolled fire that occurs where natural vegetation is the predominant ground cover. Though wildfires usually occur in less developed, rural areas, they can threaten urban environments if they are not brought under control, and they are geographically widespread.

Appendix

Inventory	XXIX
Unique Supplies Form	XXIX
Post Recovery Review	XXX
Disaster Recovery Kit Checklist.....	XXXI
Critical Business Functions Checklist	XXXIII
Critical Business Functions Form:.....	XXXV
Vendor Assessment Form	XXXVIVI
Crisis Communications Checklist.....	XXXVIII
Media Communication Guidelines	XL
News Release Template.....	XLI
Sample Voicemail Template.....	XLIII
Glossary of Terms.....	Error! Bookmark not defined.

Inventory

Unique Supplies Form

SterlingRisk has populated the below form with all unique items. This list *does not include* basic office supplies such as paper and pens, office furniture, or computers in this section.

[illegible]

Examples: including anything from special forms used for customer orders, to special toner required for a printer, to chemicals required in a manufacturing process.

Post Recovery Review

The Post Recovery Review will help SterlingRisk determine the effectiveness and improve the recovery process. SterlingRisk will plan on conducting a review both after a test and an actual recovery. In conducting a review, we will gather data and perform an overall analysis of our crisis response efforts and plan to address the following participants and/or aspects of the recovery process:

- ☐ Management team
- ☐ Support teams
- ☐ IT staff
- ☐ Personnel
- ☐ Vendors and suppliers
- ☐ Customers and/or clients
- ☐ External contacts & support
- ☐ Recovery location
- ☐ Communication (internal/external)
- ☐ Logistics and coordination
- ☐ Response time and flow
- ☐ Documentation
- ☐ Document and data storage
- ☐ Data recovery

After finalizing the post recovery review, we will complete the following steps:

Step 1.	Review evaluation and determine required changes to plan.
Step 2.	Implement changes and test.
Step 3.	Review and update your Recovery Profile and plan on myAgility.

Disaster Recovery Kit Checklist

SterlingRisk's recovery kit checklist will provide a breakdown of the items necessary to initiate recovery procedures in the wake of an interruption. One of the primary functions of our recovery kit is to protect the important records and emergency items of our business in order to ensure a smooth reconstruction of vital information and operations following any disaster.

Description	Included		Quantity	Task Assigned To
	Yes	No		
Business Continuity Plan Important Records				
Insurance Policies				
Fixed Asset Inventory				
Contracts				
Employee Information				
Operating System Installation Disks/Software Licensing Keys/Office Supplies				
Software installation disks				
Software licensing keys				
Hardware serial numbers				
Stamps				
Writing utensils & notepads				
Stapler & staples				
Tape				
Printer paper				
Calculators				
Letterhead				
Emergency Items				
Cash				
Water (one gallon per person per day)				

Map of the area				
Three day supply of non-perishable food				
Battery powered/crank radio				
Flashlight				
Extra batteries				
First aid kit				
Whistle to signal for help				
Can opener for food (if kit contains food)				
Blankets				
Sanitation				
Dust/filter masks				
Moist towels				
Plastic garbage bags				
Paper towels				
Tools				
Duct tape				
Pocket knife				
Wrench or pliers to turn off utilities				
Screwdriver				
Lighter/matches (sealed in plastic bag)				
Grab & Go Kits for Employees				
Medications				
First aid kit				
Cash				
Emergency contact information				

Critical Business Functions Checklist

Identifying critical business functions is integral in resuming operations following a disaster.

This template will walk you through the very important steps of identifying the most critical functions in your business. You may consider your critical functions as those activities that are vital to your organization's survival and to the resumption of business operations. Typically, your critical functions are the business functions that are (1) most sensitive to downtime, (2) fulfill legal or financial obligations to maintain cash flow, (3) play a key role in maintaining your business' market share and reputation, and/or (4) safeguard an irreplaceable asset. Keep in mind, the process of identifying your critical business functions will work in close conjunction with your risk assessment analysis.

Steps:

1. Identify the critical business functions of your business. Please reference the considerations below when determining the criticality of each business function.
2. Classify these critical business functions into the following categories: high (most severe), medium, and low (least severe). Please reference the proceeding graphs for an illustrated example.
3. Complete the Critical Business Functions Chart with each critical business function.
4. Attach the Critical Business Functions Chart in myAgility.

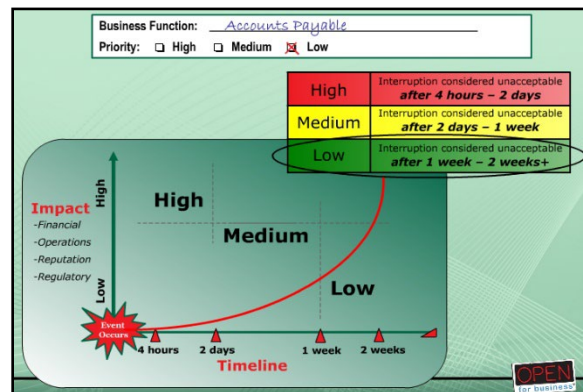
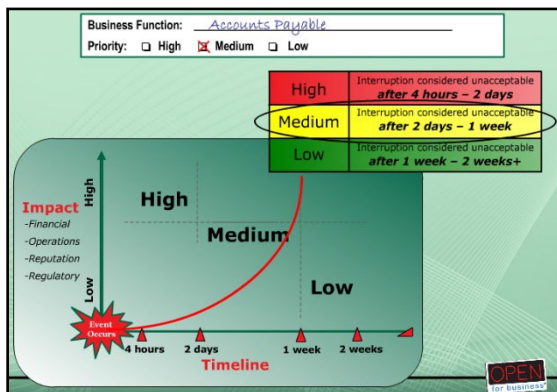
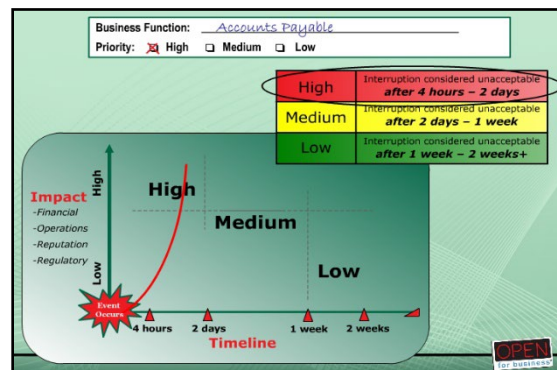
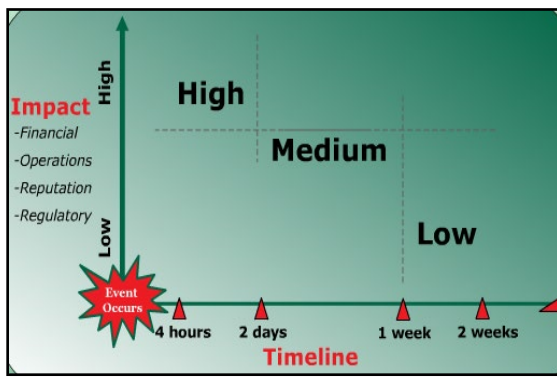
Considerations when Determining Criticality of a Function:

1. The business objective/goal this business function supports.
2. How often this business function occurs.
3. How many business units (departments) perform this business function.
4. Whether or not the successful completion of this function depends on any other business functions.
5. Whether or not other business functions are dependent on this function for their successful completion.
6. If there is a potential for significant revenue loss to the organization if this business function is not performed.
7. If there is a potential for fines, litigation, or other punishment for noncompliance due to a required regulatory requirement.
8. If noncompliance is tied to a specific downtime for this function.
9. Whether or not this function directly impacts your business image or market share of your organization.
10. The priority ranking you would give this function within the entire organization's functions.

Critical Business Function Classification

The goal of these graphs is to help you identify when it is absolutely necessary to restore each of your critical business functions. Once you have determined the maximum downtime for each function, you will be able to prioritize your list in order of most to least critical.

Consider the horizontal axis a downtime timeline and the vertical axis an impact scale. Each critical business function is going to rise over time (becoming a greater impact to your business). You can determine the impact category (high, medium, or low) of each business function by identifying which impact category the function is located in when it reaches its peak impact on your business.



Critical Business Functions Form:

Business Function:

Priority: ___ High ___ Medium ___ Low

Recovery Time Objective (Maximum downtime for function):

Employee In Charge:

Alt One:

Alt Two:

Alt Three:

Required Physical Resources for this function?

Required Personnel for this function?

Will you need more/less resources to perform this function after an isolated event vs. a regional event?

What other business functions are impacted?

Brief Description Of Procedures To Complete Function: (Consider writing procedures for short disruption and total loss)

Vendor Assessment Form

The main objective of a vendor assessment is to determine your vendors' ability to continue service despite any sort of interruption in normal operations. This could include their ability to respond during an interruption to your organization or within their own organization.

It is important to complete this assessment for each of your critical vendors so you can understand the level of risk that each poses and plan for alternatives in the event of a recovery. Once completed, store this document in the "Supply Chain" section on your myAgility account. You can attach the document directly to the record of information related to each vendor for which you complete a vendor assessment.

Step 1: Determine who is a Critical Vendor

A "Yes" to any of the statements below would classify this vendor as critical. There may also be vendors who don't meet one of the criteria below, but could still be a critical vendor. If this is the case, put the reasons under "Special Circumstances."

Vendor Name:		
Vendor Business Description:		
Contact Name:		
Contact Phone:		
Contact Email:		
Address:		
City:	State:	Zip:

Question	Y/N	Notes
Has access to critical company data		
Performs one or more critical business functions		
Has access to sensitive/confidential customer data		
Has direct impact on revenue or expenses		
Directly impacts your ability to perform one or more critical business functions		

This vendor is the only one who can provide this product/service		
--	--	--

Special Circumstances: Another reason, or special situation where this vendor may be critical to business continuity.

Critical Vendor? (Y/N)

Step 2: Determine the Level of Risk this Vendor Poses to your Organization

The following characteristics for the vendors should help you determine the level of risk each critical vendor carries to your organization.

- Has customer support that is highly available (i.e. 24 hour support)
- Insurance coverage is adequate
- Business continuity plan in place and updated at least annually
- Information security policy meets our organizational standards
- Free of negative publicity
- Will remain financially viable for the foreseeable future
- Is SAS70 certified
- Has a clearly defined service level agreement with our organization
- Provides a guarantee for availability
- Contractual terms are consistently met or exceeded
- We have timely access to another vendor(s) that can provide the same product/service for us
- A non-disclosure agreement is in place between parties

Vendor Assessment Summary – detail your plans to build a strategy with this vendor to mitigate risks during a recovery:

- Step 1
- Step 2
- Step 3
- Step 4
- Step 5

Crisis Communications Checklist

During an emergency, it is imperative that those within your organization know how to communicate effectively. This includes both internal and external communications. The following checklist will highlight some recommendations for developing and executing a well-rounded communications strategy in the face of any disaster scenario.

✓	DEVELOPING YOUR COMMUNICATIONS PLAN
	Establish a Crisis Management Team, and those within that group responsible for Communications
	Develop and regularly update an Emergency Contact List to include: <ul style="list-style-type: none"> • Home Phone • Alternate Mobile • Personal E-mail • Family Contact Information • Evacuation Plan
	Set up an Alert Notification System capable of multiple means of communication to employees, stakeholders & clients. TEST regularly.
	Ensure that employee, vendor & supplier mobile voice communications are not reliant on a single network. Utilize multiple carriers and train all critical personnel on the use of text messaging.
	Establish a separate, formal notification plan for employees' immediate families and close relatives in the event of loss of life, missing personnel, etc. Additionally, ensure that caregivers and daycare operators upon whom employees depend on can receive appropriate information.
	Ensure that a formal system exists to integrate new hires into the Crisis Communications Plan
	Consider establishing a public hot line, or a "dark" Website that can be activated on short notice to provide information during an emergency to everyone in the community
	Consider an Online Social Networking Platform for web-based crisis communications (Facebook, Twitter, LinkedIn, etc.)
	Establish a universal and easily accessible database of information about the company. Database should include company background information, critical documents, key contacts, passwords, etc.
	Consider setting up a password-protected online message board specific to your organization
	Establish remote hosting for your corporate website <ul style="list-style-type: none"> • Ensure proper bandwidth capability for spikes in traffic during crises • Ensure remote access to your website, and establish a team to manage updates to the site during disasters
	Develop a tactical response plan for Voice/Phone redirection
	Establish processes & plans to re-establish your network connectivity <ul style="list-style-type: none"> • E-mail • Core Processing • Virtual Private Network (VPN) • Remote Services
	Coordinate all Crisis Communications Planning with key vendors and suppliers to ensure seamless transition
✓	DEVELOPING YOUR COMMUNICATIONS PLAN
	Develop and test your Media Communications Strategy: <ul style="list-style-type: none"> • Designate primary and secondary spokespersons.

	<ul style="list-style-type: none"> • Ensure all Employees know WHO the Spokesperson is • Arrange for media to have 24-hour access to a spokesperson. • Give designated spokespersons training in dealing with the media. • Establish a policy for all employee interaction with Media, ON and OFF-SITE • Maintain trustworthy, credible relationships with the media all of the time. If you do, the media will be less suspicious and more cooperative in the midst of a crisis. • Identify key audiences and develop a strategy for each. • Create Key Messages & Talking Points to ensure consistent message • Ensure you have a media kit at the ready containing information about your company or organization, as well as a list of approved contacts • Discuss possible problem areas and potential negative impacts
	Identify main media outlets through which information about your organization will be disseminated (Radio & TV stations, print media, etc.)
	Find a signage vendor with multiple regional locations to use for signage needs after a disaster
✓	DURING THE CRISIS
	Have all employees, vendors, client & media contact information on hand.
	Be the first to break the news about how your organization is responding. Even if the situation is still evolving, begin with full disclosure. ALWAYS respond to media requests.
	Continue to communicate with all key audiences until the crisis has passed. Consistency is important.
	Continuously monitor online and offline conversations in order to evaluate the strengths and weaknesses of your strategy and messaging.
	NOTHING is “off the record.” Confirm facts; communicating openly and accurately about the situation. Your communications team must know the proper, approved messages.
	During evacuation have a central point of contact for all employees, and ensure you know where your people are located.
	During evacuation consider your phones lines - redirection to cell phones, answering service, Google Voice, or Agility lines could be critical.
✓	AFTER THE CRISIS
	Following the crisis, notify all critical people of next steps.
	Learn from the experience and anticipate the next crisis. Plan for likely and even unlikely scenarios based on this most recent crisis, and know the steps you’re going to take before you have to take them.
	Debrief staff on their experiences, praising people for what went well.
	Improve your plan as needed, and aim to regularly update it, including response to lingering fallout from the most recent crisis.

Media Communication Guidelines

Identify Crisis Communication Team

The Crisis Communication Team CCT (CCT) will be responsible for communicating SterlingRisk's position to key contacts and the media. The CCT may include: CEO, public relations manager, vice presidents or senior managers from key departments, company lawyer(s).

Designate a spokesperson

SterlingRisk has identified a single point of contact for the organization. They will be the face of the organization throughout the crisis and offer statements from the organization and answer questions directed from key contacts and media. SterlingRisk has also identified a backup should the primary spokesperson be unavailable for any reason.

Spokesperson: David Sterling - CEO

Alternate Spokesperson: President

When being interviewed or giving a speech:

- Speak confidently and clearly
- Answer only the questions asked and be as concise as possible
- Maintain control of the interview
- Stay on message
- Set a time limit in advance
- Ensure you're prepared with details
- Remain professional
- Avoid jargon or industry expressions
- Don't answer inappropriate questions, but instead say it is "not an appropriate topic for you to address at this time," or "it's proprietary"
- Do not speak "off the record"
- Be prepared for interruptions with questions

Prepared Statements

By being very pro-active with communication in a crisis, SterlingRisk will have the greatest influence on how the media and public view the situation. SterlingRisk will develop templates with prepared statements which will be helpful for providing the timeliest response in the midst of a crisis. They will also help to ensure that key publics receive the organization's perspective of the crisis.

News Release Template

Sample: A (what happened) at (location) involving (who/what) occurred today at (time).
The incident is under investigation and further information will follow.

Voicemail Template

Approved Voice Message (for redirection strategy):

Thank you for calling SterlingRisk. Our office is currently closed due to a (explain situation). Updates will be issued throughout the day via (method of communication: radio, website, etc.). If you are an employee of SterlingRisk, please be advised that you will receive communication about future company operations and functions as they become available. If you are a member of the media, please contact our Communication Coordinator at ... If you are a concerned family member or friend of SterlingRisk, please contact xxx at xxx. For all other urgent messages, please contact our Administrative Coordinator at xxx, or leave a voice mail.

Addendums

Addendum Name	Description
Addendums A1&A2 – Employee Contact List	Full listing of SterlingRisk Employees along with relevant contact information.
Addendum B – Vendor Contact List	Listing of critical Vendors along with relevant contact information.
Addendum C – Software Inventory	Listing of critical Software applications & versions.
Addendum D1 – D5 License Summaries	Listing of software license information for vendors such as Microsoft & Symantec.
Addendum E – Critical Hardware Summary	Listing of Critical Hardware, including Firewalls & Servers.
Addendum F – Remote Site Info	Detailed information about remote offices, their critical vendors and network information.
Addendum G – SterlingRisk Evacuation Plan	Evacuation plan for SterlingRisk Main Office in Woodbury NY.
Addendums H1 – H3 Procedure Manuals	Procedure manuals for performing department specific tasks in Agency Management Systems.