****

**IT PANDEMIC**

**BUSINESS CONTINUITY PLAN**

This document serves as protection for employees, customers, assets & information, and will minimize restoration time in the event of a pandemic. 28 Pages 47-493

**We strive to continually update our Document Library for the benefit of our Members. Please consider contributing documents from your organization.**

**Thank you!**

These documents have been voluntarily contributed by NOREX Members with the full knowledge that other Members may use them in any manner they see fit. NOREX and its Members shall not be held liable for any statements or interpretations contained within the documents.

***Information Technology***

**Pandemic**

**Business Continuity Plan**

Confidentiality Statement

This document contains confidential and proprietary information and is the sole property of [ORG]. The document or its contents shall not be disclosed, distributed or copied without the written permission of [ORG].

Document Change History

This chart contains a history of the revisions applied to this document.

| **Version** | **Author** | **Description of Version** | **Issue Date** |
| --- | --- | --- | --- |
| *1.0.0.0* | *(name)* | *Minor updates and signature* |  |
| *0.0.0.1* | *(name)* | *Minor updates to Communication plan and prioritization table* |  |
| *Draft* | *(name)* | *Initial draft created for distribution and review comments* |  |

Change Approval Document

The business owner/sponsor agrees that the changes stated in the Document Change History on the previous page have been completed and all plan documents are properly stored on the Business Continuity Planning SharePoint Site.

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue Date** | **Business Owner/Sponsor** | **Title** | **Date** |

Confidentiality Statement

Document Change History

Change Approval Document

Table of Contents

Business Continuity Plan Assumptions

Crisis Management Plan

Instructions for Addressing Media Questions

Section 2 – Business Unit

Business Continuity Plan (BCP) Administration and Maintenance

Responsibility

Approvals

Maintenance

Distribution

Business Impact Analysis (BIA)

Section 4 – Pandemic BCP

IT BCP Coordinator

IT BCP Team

Escalation Procedures

IT BCP Phase 1 (Pandemic Alert)

IT BCP Phase 2 (Pre-Pandemic)

IT BCP Phase 3 (Pandemic Outbreak)

IT BCP Phase 4 (Maximum Disruption)

IT BCP Phase 5 (Prolonged Recovery)

Section 5 – Information Technology Disaster Recovery Plan

Section 6 – Plan Tests and Results

APPENDIX A – Glossary & Terms

APPENDIX B – Internal Contacts

APPENDIX C – Vendors and External Contacts

Appendix D – Equipment List

APPENDIX E – Software List

APPENDIX F – Supplies List

APPENDIX G – Telecommunication Needs

APPENDIX H – Critical Information List

APPENDIX I – Offsite Storage

APPENDIX J – Recovery Site Information

Section 1 – Assumptions CMP/Media

POLICY

It is the policy of [ORG] to develop and maintain a Business Continuity Plan that will provide the enterprise with every opportunity to withstand a catastrophic event. Whether accidental, man-made or natural, the goal is to resume critical operations quickly and effectively. The plan is designed to minimize the effects of a disaster through pre-planning and contains actions to be taken should an event occur, with or without warning. Its primary purpose is to provide for an orderly, timely resumption of business operations by clearly defining the resources, equipment, supplies and documentation required to execute the plan, as well as roles and responsibilities in the recovery process.

SCOPE

The Business Continuity Plan is to be executed only after any immediate life-safety issues are addressed. [ORG] recognizes the need to establish comprehensive business continuity policies to protect employee health, life and safety. Although no plan can be written to address every possible type of disaster, this plan is intended to be used as a procedural resource during a disaster.

OBJECTIVE

[ORG] recognizes the need to establish comprehensive Business Continuity policies to protect employees, customers, assets and information as well as to minimize the time it will take to restore critical operations, functions, products and services after an emergency is declared. It will delineate the business impact of the disaster based on the ability to deliver energy to our customer or to support mission-critical services. The plan also facilitates the identification of resources required to resume business operations at a survivable level. The following list includes the main objectives of the plan:

* Define mission critical processes using a Business Impact Analysis
* Define critical internal resources
* Define critical vendors and suppliers
* Define the vital inputs and outputs of the business processes such as equipment, software, supplies and communication requirements
* Establish comprehensive procedures to plan for and respond to business disruptions
* Document planned and unplanned tests of business disruptions and capture the test results

Crisis Management Plan

Businesses today face a wide variety of operational, financial and reputational risks as a result of business disruption. Potential threats may include such things as power failure, computer virus, pandemic, kidnapping, extortion, political unrest and natural disaster. Any of these events could possibly create a crisis situation, requiring immediate action by the company’s senior management.

In order to better prepare for the threats of business disruption, [ORG] has implemented formal procedures for responding effectively to emergency situations in the Crisis Management Plan. A Crisis Management Team, chaired by the Chief Operating Officer, has been designated to fulfill the obligations of the plan. Although members of the Crisis Management Team are responsible for recommendations and advice in his or her specialized field, as a whole, the team is also responsible for managing through the crisis and affecting decisions in the interest of the company.

Responsibilities of the Crisis Management Team include but are not limited to:

* Monitor the status of current events and crisis that impact [ORG] operations, employees and facilities
* Make decisions in response to a crisis
* Liaise with senior management
* Declare a state of emergency
* Activate emergency action plan and establishes contact with business unit crisis teams
* Ensure timely and accurate communication to employees
* Control the content, timing and method of delivery for all news media statements
* Ensure compliance with insurance requirements including coverage to obtain reimbursement of funds disbursed during a crisis
* Establish contact with appropriate governmental and health agencies
* Establish emergency and law enforcement contact lists
* Compile and maintain comprehensive contact information for all CMT members
* Ensure the maintenance of payroll and benefits during a crisis
* Develop plans to meet the needs employees and their families during a crisis
* Determine the financial consequences of a crisis
* Ensure the availability of funds to meet contingencies
* Examine the legal consequences of a crisis and determines corporate legal responsibilities
* Ensure that all decisions and actions taken by the Crisis Management Team are in compliance with federal, state and local laws

Instructions for Addressing Media Questions

The following information is consistent with the Corporate Crisis Communications Plan:

The Crisis Communications Team will be responsible for the overall communications for emergency or crisis situations. This team will work closely with state leadership, on-site management and other designated business unit leaders to centrally coordinate all communications and confirm that all guidelines are followed.

The team will handle company-wide emergencies and/or incidents that occur at corporate headquarters, as well as local emergencies that involve death, injury or have potential impact beyond the immediate local area but do not present a major ongoing crisis situation requiring ongoing decision-making by [ORG] senior management. The team will work closely with local leadership during local emergencies and ensure that an appropriate spokesperson is identified.

In all major crisis situations, the Crisis Communications Team will coordinate all internal and external communications.

During an incident, there will be a period during which the news media may try to contact employees at the site of the incident, prior to the arrival of the official spokesperson. The following procedures are designed to cover the field situation until the official spokesperson is on the scene. Each individual location should also have a communications plan in place and all employees should be trained in the plan. The senior associate on location or a designate should serve as the interim representative to respond to the media. That individual should adhere to the following rules:

* Greet any member of the media and identify yourself as the person representing the company.
* Explain that the official spokesperson is on the way and that the company is gathering information about the incident and will release it to the media as quickly as possible. The interim or “holding” statement may simply be: “We have just heard about this matter. We are investigating and as soon as we have any information to report, we’ll let you know.” This shows concern and action on your part. It also gains time for you to gather facts and make decisions.
* Refer the media to [ORG] Communications 24-hour hotline ((number)).
* If the incident occurred, or is occurring on company property, do not permit the media on the property. Explain that a decision based on safety, security, and other factors will be made by the communications representative when he/she arrives, and that the company will do its best to provide the media with access as soon as possible if appropriate. Do not attempt to interfere with any actions of the news media on public property surrounding the company property. It is their right to be on public property, to do what they want, and to talk to whomever they want. This would also be true if the situation occurred in a public location such as a city street or a highway.
* Under no circumstances make any speculations or comments as to what happened or why it happened. Do not release any names of people other than your own. Refer all other questions to the telephone number listed above. Explain that the company values its credibility with the media and does not want to lose credibility by releasing unverified information.
* Use common sense and remain courteous despite demanding media interest

Section 2 – Business Unit

Information Technology (IT) has completed a Business Impact Analysis. These are stored on the “K” workgroups drive under the Pandemic folder. They will be reviewed and updated annually or if there are significant changes to the functions IT performs for the company.

Information Technology’s (IT) role in the business is to maintain the integrity, reliability and availability of all information technology systems that support all cash flow, financial reporting, customer satisfaction, employee well-being, regulatory reputation and utility reliability for [ORG].

Some of the provided services:

* Business Applications Support
* Critical Infrastructure support (servers, storage, databases, system software). This includes day to day operational support as well as architecture design and capacity planning.
* All corporate data base administration and management
* Data Communications Support and maintenance (WAN), enterprise communications (email, vmail), call center technology support (IVR, CTI, PBX, other call center technologies)
* 24X7 Network monitoring of all critical sites
* 24X7 monitoring of all critical infrastructure
* Customer service and support (IT Helpdesk, deskside support)
* Information Security management
* Network Security (firewall / perimeter)
* Disaster Recovery planning and services related to technology
* Business Contingency planning related to technology
* Project Management Office, consulting and training
* IT steering team leadership
* Sarbanes Oxley compliance and administration (IT operations, development, security and change management)
* IT Governance (technology standards, policies, strategic planning)
* Six Sigma technology support and services

 The organization and staffing of Information Technology can be viewed at (site).

In order to provide disaster recovery services to the business, Information Technology utilizes the services of (location) for offsite backup tapes. Backups are taken daily and one copy of the backup is sent offsite daily. IT also has a contract with [NAME] to provide a site and hardware for us to use in the event of a disaster. If there should be a disaster, [ORG] would call [NAME] at 1-800-[NAME]-SERV and declare a disaster. At that time, [NAME] would assign us a disaster recovery site. Then [ORG] would hire FedEx custom critical white glove service (1-800-255-2421) to retrieve the tapes from (location) and take them to the [NAME] assigned site.

Section 3 - Business Continuity Plan (BCP)

Administration and Maintenance

Responsibility

The BCP plan is the responsibility of the Technical Planning Manager. BCP plan administration consists of oversight, updates, distribution, and periodic review.

**Approvals**

Approval of the BCP plan will be performed by the Vice President IT as evidenced by the signature on the acceptance page (appendix K).

**Maintenance**

Maintenance of the BCP plan is the responsibility of the Technical Planning Manager. It will be reviewed and practiced during the onsite DR test which is performed annually before the offsite testing of the disaster recovery (DR) plan. Testing will be conducted via a tabletop exercise.

**Distribution**

Any BCP plan updates will be distributed by the Technical Planning Manager to the Vice President IT and the IT Directors. BCP test results will be distributed to the IT ELT.

**Business Impact Analysis (BIA)**

The BIA will be reviewed annually at the same time as the BCP plan is reviewed. Any updates or distributions will be handled in the same fashion as the BCP plan.

Section 4 – Pandemic BCP

**IT BCP Coordinator**

The Technical Planning Manager is the BCP coordinator. If the Technical Planning Manager is unable to fulfill his responsibilities the first alternate will be the IT Infrastructure Director. The second alternate is the IT Communications services Director.

**IT BCP Team**

The IT BCP team shall consist of the Vice President IT, the IT Directors, and the Technical Planning Manager. The following table shows the team and their alternates. Should one of the team become ill, they are responsible for notifying their alternate.

|  |  |  |
| --- | --- | --- |
| **Name** | **Area of responsibility** | **Alternate (Primary & Secondary)** |
| (name) | All of IT | (name) & (name) |
| (name) | Infrastructure & Operations | (name) & (name) |
| (name) | Applications | (name) & (name) |
| (name) | Network & Telephony | (name) & (name) |
| (name) | Security | (name) |
| (name) | Plan Administration | (name) & (name) |

Escalation Procedures

*[ORG]’s pandemic business continuity plan follows the North American Electric Reliability Council (NERC) phase designations, which correspond to the phases established by the World Health Organization (WHO). This is not to say that [ORG]’s enterprise plan will be activated at the same time that the severity level is elevated by the WHO. The decision to activate [ORG]’s pandemic business continuity plan will be made by the Crisis Management Team when absenteeism or other situations warrant an elevation of status. The Crisis Management Team Chairman will issue the declaration and subsequently notify the Leadership Team, the state Vice Presidents, and the Extended Leadership Team. In turn, these managers will issue the directive to activate the departmental pandemic plans in their respective areas.*

IT BCP Phase 1 (Pandemic Alert)

* Assemble a team to begin planning for business continuity in the event of a pandemic
* Monitor progression of the virus
* Research preparation strategies for businesses and home

IT BCP Phase 2 (Pre-Pandemic)

* Monitor progression of the virus
* Identify critical processes, functions and responsibilities
* Identify essential and non-essential personnel. Prepare to function with only essential workers on site, and others working from home. For essential staff, identify those who must work on site and those who could telecommute. For telecommuters, enable their network access and assess need for additional equipment at home.
* Consider sequestering employees in critical functions
* Update emergency contact information for all personnel
* Develop the pandemic business continuity plan
* Develop a communication plan to manage employees before, during and after an outbreak
* Prepare for conference calls at pre-arranged times on a daily/weekly basis
* Assess need for personal protective equipment
* Evaluate the need for stocking supplies
* Plan for absenteeism
* Cross-train employees in critical functions and consider resource sharing
* Develop a succession plan to identify individuals to step up in case others cannot perform their duties
* Review authorization levels for backup personnel
* Review contractual obligations and write pandemic clauses into new contracts
* Anticipate post-disaster needs
* Test the plan regularly
* Dispense Personal Protective Equipment.

IT BCP Phase 3 (Outbreak)

The Information Technology plan does not change when [ORG]’s Crisis Management team changes the phase from Phase 2 (Pre-Pandemic) to Phase 3 (Pandemic Outbreak).

HR will be sending out new policies with phase 3. Managers will need to inform their direct reports of the new policies. IT will abide by these new policies as well as any additional policies, guidelines or directives issued by any other parts of the corporation.

During phase 3, it will be the responsibility of the Vice President of IT (who is a member of the [ORG] Crisis Management team) to keep the IT Business Continuity team informed of upcoming changes to the situation.

During phase 3, (name) or her backup will update the IT portion of the recorded message for [ORG] employees. This message will be activated at the beginning of phase 4.

IT BCP Phase 4 (Pandemic Outbreak)

When the [ORG] Crisis Management team changes the phase from Phase 3 [pandemic outbreak] to Phase 4 [Maximum Disruption], the Vice President of IT will issue a directive that the IT Pandemic Business Continuity Plan is being implemented. When this directive is issued, a series of parallel activities will commence.

The VP of IT or his designate, will send an email (address) to all IT instructing them to go home if they are already at work or stay home if they are not as IT is implementing a work from home strategy until such time as the directive is reversed.

The phone message which (name) recorded during Phase 3, will be activated by someone out of the PBX support group. Should the message need to be updated, (name) or her backup will be responsible for updating this message accordingly.

The Director of infrastructure or his designate will send an email (address) to all [ORG] informing them the IT Pandemic BCP plan has been implemented. This email will state how the preferred method of getting a help desk ticket should be via an email to the IT Support Center as the phones will be going to voicemail which will be retrieved and processed at least once per shift. This email will also state that IT is implementing a change moratorium until further notice. The third item this email will cover is that end user support will respond as best they can, given the existing circumstances. The fourth item addressed by the email will be the immediate change of voice mail retention from 30 days to 14 to ensure there is enough room for all the voice mails anticipated to the critical corporate response phone numbers.

The VP of IT starts a call tree by calling his directors. At this point in time, things are put on hold until the new policies are issued by HR. At that time, the VP of IT will then contact the remaining of his direct reports and the directors will call their direct reports who will call their direct reports, etc. until everyone in IT has been notified of the status and what their roles will be during the pandemic. It is important that the person placing the call explain the new HR policies and role the caller is expected to fulfill during the emergency. Should the manager have a contractor working for them, they are responsible for informing the contractor of the new status.

As always, IT’s primary responsibility is to keep the production systems running. It is up to the individuals to ensure their management knows if they have become ill or cannot perform their job duties for other reasons. It is up to IT management to ensure the call out list is kept up to date (address).

The daily (M-F 8:30 AM) operations phone call will continue during the pandemic. The call in number is 1- 866- xxx- xxxx & the Passcode is \*xxxxxxxxxx\*. As usual, it is the responsibility of operations to lead this meeting. Since there is a change moratorium in place, the change control portion of the meeting is cancelled until further notice.

The Vice President of IT and each of his directors are responsible for determining who in IT is available to work daily by 9 AM. Daily at 9:00 AM the Vice President of IT and his directors will get together via conference call (**1-866-xxx-xxxx - Pass code \*xxxxxxxx\* – Call originator will need to start the meeting with the following PIN: \*xxxx\***) to work out where resources are needed to get through the current day’s issues. Should a director be unavailable, he is responsible for assigning an alternate to fill in for him during his illness. After this phone call, the Vice President of IT is responsible for informing the [ORG] Leadership team of the state of IT on a daily basis.

A number of critical phone numbers will be used by [ORG] during this time. To be able to accommodate setting up larger voice mail repositories for those critical numbers, it will be necessary to reduce the voice mail retention for all other voice mail boxes to 14 days. This will be implemented by the telecom group.

If an IT employee receives invoices via the USPS, they are responsible for ensuring those invoices get processed. Should the employee be unable to work, they should inform their manager or his alternate about these invoices to ensure payment. Accounts Payable is going to automatically pay invoices as they come in. It will be up to the manager to clean up any issues caused by this during Phase 5 (Prolonged Recovery).

There are certain vendors who IT works with on a very frequent basis. These vendors should be informed of [ORG]’s status. The following is a list of vendors, vendor contacts, and who is responsible for contacting them.

|  |  |  |  |
| --- | --- | --- | --- |
| **Vendor** | **Vendor Contact** | **[ORG] Contact** | **Phone Number** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

All IT employees continue to be responsible for updating their voicemail message appropriately and for checking voicemails regularly. Should the IT employees wish to have their phone messages forwarded to their home or cell phones; there is a facility which is being tested. To access this facility:

Please use this URL -

1. Your MAILBOX NUMBER is your 4-digit extension
2. The TELEPHONE NUMBER FOR VOICE PLAYBACK is the specific telephone number you would like the system to call so you can hear your VMs (e.g., home #, cell #, etc.). Please note you must use the actual 10-digit number.
3. The PASSWORD is your actual voicemail password.

IT employees with access to the (name) Data Center have been given N95 masks and gloves to use at their discretion. If they need to meet someone at the data center who could be infected, they are encouraged to use these masks and gloves.

IT employees who work in End User Support have also been given N95 masks and gloves to use at their discretion. If they need to go to someone else’s cube, they are encouraged to call Facilities and ask that the cube be treated with UV Band C and to use the N95 masks and gloves. Since a large number of [ORG] employees will be working from home, End User Support will make every attempt to help the person on the phone, however, since it will probably not be company issued equipment, the support they can offer will be limited.

Face to face meetings should not be held. If meetings are required, use of the (name) and (name) conference bridges is encouraged. Should they not be available or not have enough lines, contact your Director to use one of their assigned conference call numbers. If those are not available, feel free to use the Verizon conference calling facility to establish a conference call. The following link has step by step instructions for establishing a conference call.

(insert link)

Should there be a resource conflict; the following table will be used to assist in prioritizing tasks

**IT Problem Resolution Prioritization**

|  |  |
| --- | --- |
| **Priority** | **Business Function** |
| 1 | Procure, transport and store electric generation fuel |
| 2 | Operate and maintain generation, transmission and distribution systems (gas and electric) |
| 3 | Hiring, separation and payment of employees, contractors and suppliers |
| 4 | Produce, procure and dispatch energy |
| 5 | Transmit and distribute energy (power) |
| 6 | Timely & accurate response to customer inquiries |
| 7 | Procurement, stocking and distribution of non-fuel supplies (includes poles, wires, pipes, warehouse inventory) |
| 8 | Metering, billing and collection of revenues |
| 9 | Preparation and timely dissemination of accurate financial statements |
| 10 | Ensure compliance with financial covenants |
| 11 | Compliance with laws and regulations |
| 12 | Timely filings with regulators and the judicial system; Resolution of legal and regulatory issues |
| 13 | Timely communication with customers, employees, investors, regulators, communities and legislators |
| 14 | Applicable to Enterprise |

As phase 4 starts to weaken and things stabilize, IT leadership will start to plan how they are going to manage the return to work of people in phase 5.

IT BCP Phase 5 (Prolonged Recovery)

The Information Technology pandemic business continuity plan does not change when the Crisis Management team changes the phase from Phase 4 (Maximum Disruption) to Phase 5 (Prolonged Recovery). However, the Vice President of IT and his Directors should start planning returning to normal. This may involve hiring personnel, and reassigning the people returning to work. This phase should involve significant direction from the senior leadership team and the [ORG] Crisis Management Team in terms of how stable the company is financially, how the progression of the pandemic has slowed, and how soon [ORG] will have to get back to normal in terms of requirements for SOX testing, etc.

Section 5 – Information Technology Disaster Recovery Plan (DRP)

Information Technology does an annual Disaster Recovery test. This test consists of recovering certain applications at a remote site using the backup tapes which are sent off site daily. This plan is currently being rewritten due to the entire infrastructure hardware being right sized. There will be a link in this section to the rewritten plan once it is completed.

Section 6 – Plan Tests and Results

APPENDIX A – Glossary & Terms

APPENDIX B – Internal Contacts

APPENDIX C – Vendors and External Contacts

Appendix D – Equipment List

|  |  |
| --- | --- |
| **Equipment** | **Specifications** |
| Workstation | Computer (desktop or laptop) - monitor, keyboard and mouse included |
| Telephone | Phone for conference calls and communicating |
| Cell Phone | Cell phone to contact personnel anywhere / anytime |
| Phone Headset | Headset to work while communicating with personnel |
| Key fob | Secure method to access [ORG] network for support |
| Chair | With a seat and back, adjustable |
| Desk | Work area |
| Printer | Copy machine |
| Copy Machine | Xerox |
| Fax Machine | Xerox |
|   |   |

APPENDIX E – Software List

|  |  |
| --- | --- |
| **Software** | **Specifications** |
| Chrome web browser | Navigate Internet, manage systems |
| [ORG] Home page | Reference company information |
| Outlook | Communications |
| [ORG] Directory | Employee Lookup |
| Windows | Windows 10 |
| Microsoft Office | Client software, server software, services |
| Microsoft Word | Documentation |
| Microsoft Excel | Calculation and documentation |
| PeopleSoft | Enter Timesheet |
| PVCS Tracker | Enter Change Controls |
| Visio | View Architecture Diagrams |
| Office 365 | Cloud based subscription service |
| SharePoint | Document management, storage, collaboration |
| Adobe Reader | View PDF Files |
| Windows Messenger | Instant communication amongst peers |
| Winzip | Open, extract archives |
| DNS | Add / remove addresses  |
| Active Directory | Update account information |
| Oracle Tools | Manage databases |
| SQL Server Tools | Enterprise Manager to manage databases |
| BEA Console | Manage Web Application environment |
| Putty | Remote access to Linux/HP-UX environments |

APPENDIX F – Supplies List

|  |  |
| --- | --- |
| **Supplies** | **Specifications** |
| Tablets | Any type of writing tablet for notes |
| Pens | Black Ink Pen |
| Highlight Markers | Highlighting text |
| Paper Clips | Small and large |
| Tape | Scotch Tape  |
| Stapler | Stanley Bostitch 2000 |
| File Folder | Letter Size |
| Paper | 8x11 printing paper |
|   |   |

APPENDIX G – Telecommunication Needs

|  |  |
| --- | --- |
| **Telecommunication Requirements** | **Specifications** |
| Cell Phone | With text messaging and internet capabilities |
| Telephone | Avaya or any model that works |
| Pager | Any paging type device |
| Phone Card | Used for making long distance calls from home |
|  |  |

APPENDIX H – Critical Information List

|  |  |  |  |
| --- | --- | --- | --- |
| **Description** | **Location** | **Who is Authorized to Access** | **Criteria for retrieval and management of Information** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

APPENDIX I – Offsite Storage

(location)

APPENDIX J – Recovery Site Information

[ORG] has a recovery contract with [NAME]. Our customer number is xxxxxxxx. Our BCS schedule number is xxxxxxx.

In the event of a disaster, VP of IT shall call 1-800-[number] to declare a disaster. Both of the above numbers will be needed.