

SAMPLE
Disaster Recovery Plan - PART
Table of Contents

1. *Notification Process*2
 1.1. Declaring a Disaster.....2
 1.2. System Unavailability Notification.....3
 1.3. System Recovery Notification3
2. *Recovery Process*.....4
 2.1. Diagnostic and Recovery Activities.....4

1. Notification Process

System unavailability and recovery notification process described below explains how the System Custodian and System Owner approve a disaster declaration and how key contact and users will be notified. Notification may be via phone, voice mail, email, fax, or face-to-face communication.

1.1. Declaring a Disaster

General Description: If the system is down as the result of an FTP server failure, an emergency is considered to have occurred when the system will be down for more than 48 hours. In the case of a fire or natural disaster, an emergency is considered to have occurred if the system will be down for more than one month. In the event of an emergency, the recovery team will take action as indicated. The System Custodian or System Owner declares a disaster.

The following events may trigger a disaster.

- Hardware issues arise where the hardware, operating system or other platform component is rendered unusable or unstable necessitating a migration to an alternate system
- Physical destruction or degradation of the hardware or of the facilities where the hardware resides
- As a correction for otherwise unresolved load-balancing or intolerable performance issues

Risk	Magnitude of Emergency	Resulting Actions
FTP Server Failure	Unable to transport data files between X and Y through the use of the FTP server.	Data files would still be accessible and would be transmitted between X and Y using other methods, such as e-mail or physical CD. These data files would be loaded to the appropriate location and processing started with execution beginning immediately after the step of loading the data files to the proper location.
Fire, tornado or other natural disaster.	The disaster does minimal damage to Building 1, which is the location of the team member offices.	The team would conduct an off-site meeting. The team would initially meet at Building 1 and relocate to an off-site location to organize recovery efforts. (See the Recovery Plan section of this document.)
Fire, tornado or other natural disaster.	The disaster damages a substantial portion of Building 1, which is the location of the team member offices.	The Business Continuity Planning (BCP) Owner and caretakers would coordinate with US Demand IT and corporate BCP representatives to initiate system recovery procedures as outlined in this document. (See the Recovery Plan section of this document.)
Computer virus, internal or external sabotage or other malicious system attack.	The system shuts down.	The team would: <ul style="list-style-type: none"> • Isolate the system from the rest of the network • Remove the virus or fix areas affected by the attack • Test and place the system back into production (See the Recovery Plan section of this document.) Note: The team would neither send nor receive data from X during the time system is unavailable. The data originally scheduled for processing would be sent once the system was available and tested.
Computer virus,	Data corruption occurs.	The team would:

Risk	Magnitude of Emergency	Resulting Actions
internal or external sabotage or other malicious system attack.		<ul style="list-style-type: none"> • Isolate the system from the rest of the network • Remove the virus or fix areas affected by the attack • Test and place the system back into production <p>(See the Recovery Plan section of this document.)</p> <p>Data would be restored from the most recent point in time for which it could be verified to be without corruption.</p> <p>Note: The team would neither send nor receive data from X during the time system is unavailable. The data originally scheduled for processing would be sent once the system was available and tested. Processing would resume with data from immediately after the point in time to which the system data was recovered.</p>

1.2. System Unavailability Notification

If the system becomes unavailable, the following steps should be followed to ensure communication to the appropriate persons.

1. System Owner or System Custodian contacts the Lead Data Steward.
2. Lead Data Steward contact the Support Center, Support Analyst, Key Business Contact, and Reporting Account Manager.
3. The Support Analyst completes the initial assessment of trouble according to the corporate IT Change Management Standard Operating Procedure (SOP), initiates the required Trouble Ticket (s), and communicates to all users.

1.3. System Recovery Notification

1. When the system is recovered, the System Support Analyst performs disaster recovery testing per the testing instructions identified in the Recovery and Verification section of this document and contacts the Lead Data Steward.
2. The Support Analyst completes the Disaster Recovery Execution Report and supplies information to the System Custodian.
3. The System Custodian reviews the Disaster Recovery Execution Report, approves it, and forwards it to the System Owner.
4. The System Owner reviews the Disaster Recovery Execution Report, approves it, and forwards it to the Support Analyst.
5. The Support Analyst notifies the Lead Data Steward and communicates to all of the users when the system is available.
6. The Lead Data Steward notifies the Key Business Contact and the System Custodian (*and System Owner*).
7. The Support Analyst closes the Trouble Ticket(s).

2. Recovery Process

A disaster may render part or all of the application unavailable. The following table describes diagnostic and restoration activities that must occur if the facilities containing the system are destroyed. Based on the cause and extent of the disaster, the Support Analyst will begin executing applicable recovery activities.

The Disaster Recovery Plan and Backup and Restoration Procedures identified in this document will be used to recover and verify system components supported within corporate IT.

2.1. Diagnostic and Recovery Activities

The following diagnostic and recovery activities are needed to recover the system from a disaster.

- Database
- Software
- Hardware
- Communication
- Documentation

The following steps should be performed in the order presented below by the resource identified:

STEP	ACTION	RESOURCE
1	<p>Perform Communication Recovery Process if any recovery is to be performed. Communication needs to be sent at the beginning and the end of the recovery process.</p> <ol style="list-style-type: none"> 1. communicate the problem to the business via email or voice mail (refer to the System Unavailability Notification subsection of this document) 	System Custodian
2	<p>Create a Severity 2 Trouble Ticket (TT) in Remedy and assign to X queue. Assignee Group: XXXX</p>	Production Support Analyst
3	<p>Begin diagnostic checks to determine which area is responsible for recovery. Typically, this is performed in the following order:</p> <ol style="list-style-type: none"> 1. database diagnostics 2. software diagnostics 3. hardware diagnostics 	Production Support Analyst
4	<p>Perform database diagnostic check by first verifying that DB2 and Oracle are up and running. If so, proceed to software diagnostic check below.</p>	Production Support Analyst
5	<p>If DB2 and Oracle are not running, create a Severity 2 Trouble Ticket (TT) and assign to X Group: (Assignee Group: XXXX) --stating the issue and database impacted --instructing them that the database needs to be recovered --referencing original TT</p>	Production Support Analyst

STEP	ACTION	RESOURCE
6	<p>Once X has recovered the database and successfully closed the TT assigned to them:</p> <ol style="list-style-type: none"> 1. run incremental data load 2. refresh data 3. perform testing by running database recovery test script located in Appendix D of this document 4. successfully close out original TT assigned to 5. proceed to communication recovery step below. <p>*NOTE: If data loads fail for any reason, proceed to software diagnostic check leaving TT open while investigating issue. Note actions taken as steps are performed.</p>	Production Support Analyst
7	<p>Perform software diagnostic check by first verifying the following software applications are running correctly:</p> <ul style="list-style-type: none"> • Korn Shell Scripts • Informatica • Oracle • FTP • SAS 	Production Support Analyst
8	<p>Create a Severity 2 Trouble Ticket (TT) and assign to X: (Assignee Group: XXXX) --stating the issue and software impacted --referencing original TT</p>	Production Support Analyst
9	<p>Once the X group has restored the appropriate software and successfully closed the TT assigned to them:</p> <ol style="list-style-type: none"> 1. visually verify that the repository contains all of the source code for the system. 2. successfully close out original TT assigned to 3. proceed to communication recovery step below <p>*NOTE: If software recovery fails for any reason, proceed to hardware diagnostic check leaving TT open while investigating issue. Note actions taken as steps are performed.</p> <p>*NOTE: No formal test scripts will be created.</p>	Production Support Analyst
10	<p>Perform hardware diagnostic check by first verifying the following hardware is working correctly:</p> <ul style="list-style-type: none"> • UNIX • Mainframe 	Production Support Analyst

STEP	ACTION	RESOURCE
	<ul style="list-style-type: none"> • Windows 2000 	
11	<p>Create a Severity 2 Trouble Ticket (TT) and assign to X group: (Assignee Group: XXXX) --stating the issue and platform impacted --referencing original TT</p>	Production Support Analyst
12	<p>Once the X group has repaired the appropriate hardware and successfully closed the TT assigned to them:</p> <ol style="list-style-type: none"> 1. perform a software diagnostic check and recovery 3. perform a database diagnostic check and recovery 4. successfully close out original TT assigned to 5. proceed to communication recovery step below. <p>*NOTE: Server-level testing is the responsibility of the X team. Informal testing will consist of being able to access the data warehouse and verifying that data is present in the warehouse. No test scripts will be created for this verification effort.</p>	Production Support Analyst
13	<p>Perform Documentation Recovery Process as follows:</p> <ol style="list-style-type: none"> 1. verify hard-copy masters exist in the corporate IT Library. If all hard-copy masters are destroyed, they cannot be replaced because of the signatures acquired and the dates the masters were signed 2. verify electronic masters still exist in ClearCase. If inaccessible, contact the ClearCase representative. <p>*NOTE: If all hard copy masters in the corporate IT Library are destroyed, they cannot be replaced because of the signatures acquired and the dates the masters were signed.</p>	Quality Representative
14	<p>Perform Communication Recovery Process after the problem resolution. Communication needs to be sent at the beginning and the end of the recovery process.</p> <ol style="list-style-type: none"> 1. communicate the problem resolution to the business via email or voice mail (refer to the System Unavailability Notification subsection of this document) 	System Custodian