Information Technology Disaster Recovery Plan (ITDRP)

Document Information

Revision History:

Version #	Author Name	Revision Date	Reason for Change	Section(s) Changed / Added
0.1	Wayne Harrison	4/20/2015	Initial draft	
1.0	Wayne Harrison	9/11/2015	Updated based on feedback from doc review.	Changed Section: 1.3
1.1	Wayne Harrison	10/15/2015	Added columns to revision history table. Removed Russ Aaronson VP of Infrastructure from document; Added Rob Guinn - Sr. Director of IT-Security	Changed Revision History Table; Changed Sections 3.2, 2.1, 5.1
1.2	Wayne Harrison	11/2/2015	Removed Rob Guinn and added Paul Kohler. Updated Key personnel based on recent resignations	Changed Sections: 3.2, 2.1, 5.1
1.3	Wayne Harrison	4/19/2016	Removed Mike Polen; Added Darren Ghanayem. Updated key personnel based on recent organizational changes .	Changed Sections: 3.2,2.1,5.1 and distribution list
1.4	Wayne Harrison	9/1/2016	Annual review prior to Atlantic Hurricane Season	Changes section 1.3, 5.1
1.5	Wayne Harrison	9/15/2016	Added John Rhome as IT Director for distribution	Distribution List
1.6	Wayne Harrison	1/31/2017	Updated personnel changes and SunGard Portal address	5.1 and 6.1
1.7	Wayne Harrison	5/8/2017	Annual Review-Revised Appendix 5 to reflect current Staffing	Appendix 5 Amended
1.8	Wayne Harrison	8/2/2017	Change Bridge numbers	4.1 and 4.2
1.9	Wayne Harrison	4/2/2018	Added new IT Director. Updated listing new replication, name change for Tampa data center, personal and mission critical changes	1.3,2.1,5.1, 6.5

Document Approvals:

Version #	Approver Name	Title	Approval Date
1.1	Matthew Hubbard	Senior Manager, IT Client Services	10/16/2015
1.2	Matthew Hubbard	Senior Manager, IT Client Services	11/6/2015
1.3	Matthey Hubbard	Senior Manager, IT Client Services	4/25/2016
1.4	Matthew Hubbard	Senior Manager, IT Client Services	9/1/2016
1.5	Matthew Hubbard	Senior Manager, IT Client Services	9/15/2016
1.6	Matthew Hubbard	Senior Manager, IT Client Services	2/3/2017
1.7	Matthew Hubbard	Senior Manager, IT Client Services	5/24/2017
1.8	Matthew Hubbard	Senior Manager, IT Client Services	
1.9			

Distribution List:

Name	Title
Wayne Harrison	Technical Project Manager, IT-Client Services
Matthew Hubbard	Senior Manager, IT Client Services

Darren Ghanayem	CIO
Paul Kohler	VP- IT Infrastructure
Lydia Ophaug	Director, IT-Client Services
Jim Harrison	Manager-Infrastructure Sys. Engineering
John Rhome	Sr. Director-IT Infrastructure
Matthey Lawley	Sr. Director-IT Infrastructure

Table of Contents

1 Plan Overview

1.1 Purpose

The purpose of the Information Technology Recovery Management (ITRM) plan is to provide a structure and guidelines for command and control to quickly make critical response decisions for an IT major incident or disaster situation that results in a loss of the data center and to oversee the recovery activities conducted by the recovery teams as documented in the Infrastructure Recovery plans.

1.2 Document Scope

The scope of this document is limited to the command and control for the recovery of the data center infrastructure in all circumstances restoration of information processing capabilities and addresses events that include, but not limited to:

1. Catastrophic data corruption.
2. Complete disruption of the data center.

1.3 Recovery Strategy

WellCare has a contract with AT&T/SunGard to provide a backup data center for the WellCare corporate data center at SunGard for Tiered infrastructure and applications. At SunGard, WellCare has dedicated network, compute and storage equipment in a secured location. At time of declaration, SunGard provisions additional compute equipment.The WellCare network is present and operational in both production data center and SunGard recovery location.

WellCare utilizes a number of backup/recovery methods for data replication, server O/S and applications. SRDF(Replication), Netbackup and Data Domain technology is used to backup and restore host and data. Oracle RMAN is utilized to backup Oracle databases using various korn shells and is scheduled through the UNIX cron utility. MYSQL innobackup process is comprised of several korn shells to backup mysql databases and to clean them up. Like with oracle, the scripts are scheduled through the Unix cron utility.

The voice environment consists of servers that reside in the Cyxtera Data Center (A-Side – Tampa, FL) & the SunGard Data Center (B-Side – Carlstadt, NJ). If the A-Side were to be lost, the B-Side will automatically handle all of the voice services until services have been restored.

WellCare systems are recovered in the following order by the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) as mandated by the Business in the annual Business Impact Assessments (BIA). Refer to the section 6.5 for the Tier 1 Mission Critical Applications.

Tier 0 RTO ≤ 4hr. RPO≤ 1hr.	Tier 1 RTO ≤ 12hrs RPO ≤ 1hr	Tier 2 RTO ≤ 24hr RPO ≤ 1hr	Tier 3 RTO ≤ 48hr RPO ≤ 24hr
Basic Infrastructure components required to support critical apps (Tier1)	Critical business interactions with members and providers; Transactions from critical external parties	Critical, time sensitive business functions	Enterprise, operational efficiency and time constrained functions

1.4 Assumptions

1. WellCare has sufficient staff, with appropriate skills, available to execute recovery operations.
2. The SunGard contract is current and is aligned with the IT recovery requirements.
3. The SunGard Carlstadt data center recovery facility is available and operationally ready to use following a declared disaster event and that;
    a. Data Center equipment is configured correctly with sufficient capacity to perform data center operations after transferring operations from the primary data center (located at CenturyLink);
    b. The data communications network has sufficient bandwidth capacity for normal business operations.
4. Infrastructure Personnel supporting database restoration, technical support and application execution will be located at a WellCare IT Command Center (See step 4.0 Activate IT Disaster Recovery Command Center. All other staff will operate remote connecting to the recovery environment via VPN.
5. Vital data stored on servers and databases are backed-up and are sufficient to re-establish the business functions.
6. Emergency financial procedures for the purchase of equipment and services are expedited during the recovery process. Normal waiting periods will be bypassed in order to support rapid procurement of required components.
7. The expectation for recovery turnaround for Tiers 0 - 4 to be supported by IT is 72 hours. Only after 72 hours after disaster declaration, should the business have an expectation that systems should be available
8. Internal communications (Lync) will be available along with an open bridge for the means of communication.

2 IT Disaster Recovery Organization

The IT Disaster Recovery organization is comprised of individuals with the expertise and technical skills required to affect an efficient, timely recovery of data center infrastructure functions when a major disruption or disaster occurs.

Although the IT Disaster Recovery organization is designed to address a worst-case scenario (i.e., the data center is rendered totally unusable), The Disaster Recovery Organization is designed to provide the actions necessary to respond to, and recover from, a major disruption affecting WellCare's data center infrastructure.

The primary duties of the WellCare Disaster Recovery Organization are summarized below. Details are defined in the following sections within this document.

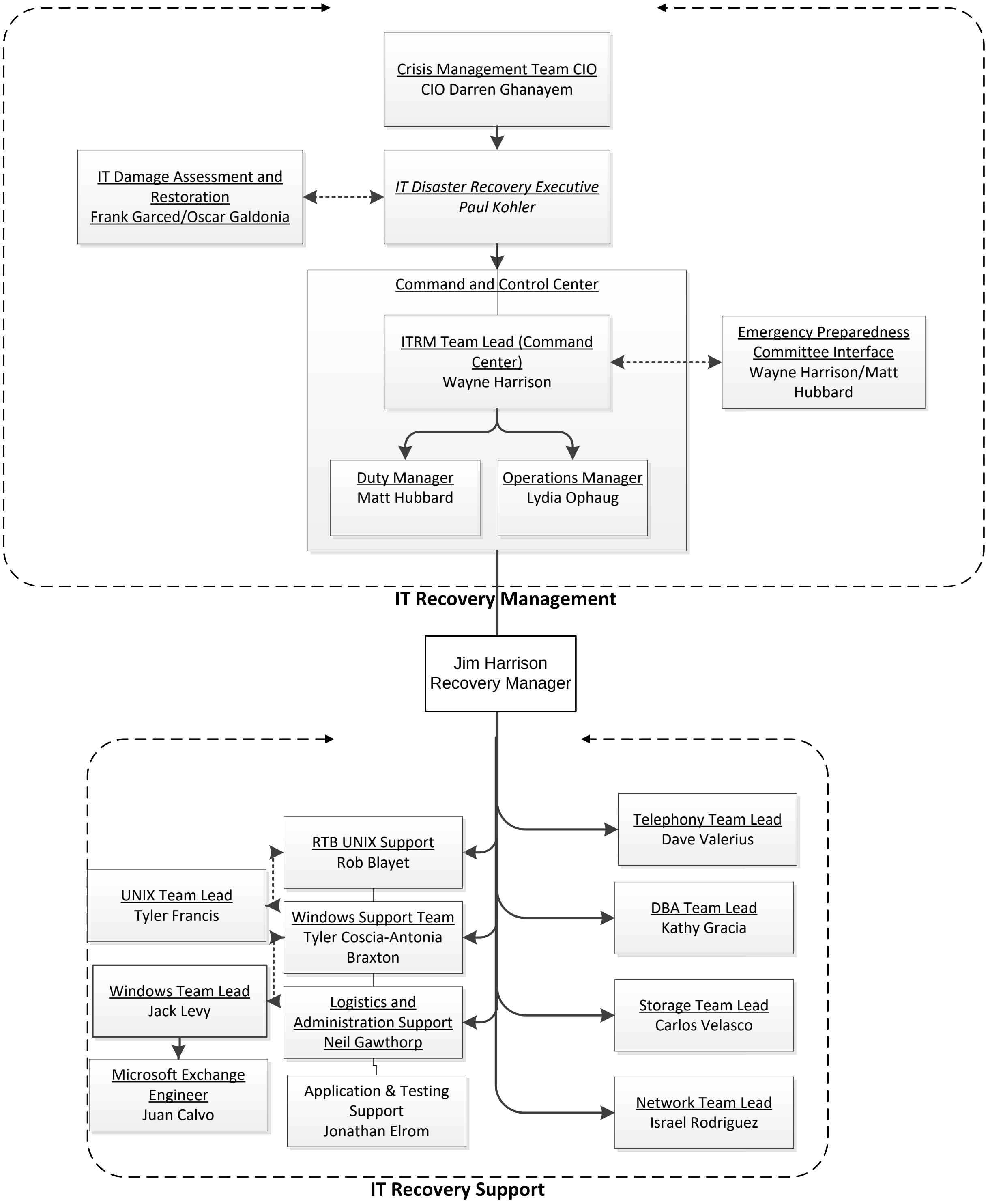
1. Ensure that the capability to recover from a disaster within specified recovery time objective is maintained as defined in the section 1.3 Recovery Strategy above.
2. Establish and maintain WellCare systems that support Tier 0-3 as supported by IT.
3. Manage recovery activities until normal operations are resumed.
4. Perform damage assessment activities (See step 3.0: Assess the Situation/Damage in section 4.2 ITRM Recovery Task List within this document.)
5. Accomplish rapid and efficient recovery of functions and operations critical to maintaining services, minimizing financial and operational impacts, and sustaining the business.
6. Exercise impact and expenditure decisions regarding critical resources.
7. Conduct status reporting of recovery progress to users and to Executive Management. (See step 7.0: Communication Information in section 4.2 ITRM Recovery Task List within this document)

The IT Disaster Recovery organization is divided into two major groups outlined below:

1. ***IT Recovery Management (ITRM)*** group provides the coordination and leadership for the day-to-day recovery activities. This group oversees every aspect of restoring data center infrastructure processes and customer services, restoring full (normal) operating capacity, restoration or replacement of the affected facility, and the planning and execution of migration of operations from the alternate site(s) to the restored/replaced facility. The ITRM team is responsible to Executive Management through the VP-Infrastructure. EPC and is led by the WellCare IT Disaster Recovery Executive.
2. ***IT Recovery Support*** group is responsible documenting the technical procedures for recovery of critical data center infrastructure and for the rapid acquisition and installation of servers, LANs, hubs, PCs and telephones at the recovery sites that will be used by business functions. This group also provides all ancillary services (except recovery of technology) for the affected data center functions.

2.1 IT Disaster Recovery Organization

The WellCare IT Disaster Recovery Organization is depicted in the following diagram:



2.2 IT Recovery Management Team

ITRM team provides the coordination and leadership for the day-to-day recovery activities. This group oversees every aspect of restoring the data center infrastructure processes and customer services, restoring full (normal) operating capacity, restoration or replacement of the affected facility, and the planning and execution of migration of operations from the alternate site(s) to the restored/replaced facility.

See previous page for the DR organizational structure and role assignments.

The primary duties of the ITRM are summarized below. Details are defined in the following sections within this document.

1. Perform initial situation assessment (See step 3.0: Assess the Situation/Damage in section 4.2 ITRM Recovery Task List within this document).
2. Recommend disaster declaration or an incident escalation plan to Executive Management through the VP Infrastructure/EPC
3. Communicate on-going event status (See step 7.0: Communication Information in section 4.2 ITRM Recovery Task List within this document)
4. Provide overall command and control of an IT event
5. Oversee and direct the actions of the IT Disaster Recovery Organization
6. Make IT infrastructure recovery decisions on behalf of WellCare
7. Monitor and report the on-going event activities
8. Determine when normal operations have returned
9. Keep records of the event and recovery process
10. Oversee damage assessment and asset replacement, salvage, disposal

2.2.1 IT Disaster Recovery Executive

- Responsible for the overall recovery from any disaster or catastrophic event
- Make the decision to declare a disaster or not based on all available information from the Damage Assessment Team and other information specific to the interrupting event.
- Manage the IT Disaster Recovery Organization as it responds to any interruption which can include:
  - Activating the Damage Assessment Team.
  - Activating the IT Disaster Recovery Organization.
  - Communicating the situation to the IT Recovery Organization Team Leaders.
  - Activating the IT Disaster Recovery Command Center.
  - Managing and coordinating the execution of the IT Disaster Recovery Plan.
  - Plan and coordinate the reconstruction or replacement of any damaged facility.
- Provide frequent reports to the VP Infrastructure/EPC and WellCare Executive Management to keep them abreast of the status of recovery and, in later stages, the restoration of the original site.

2.2.2 ITRM Team Lead

- Maintain overall control and direction of the disaster recovery effort
- Remain in contact with all functioning recovery teams
- Serve as a point of contact for all team leads for the reconciliation of resources and schedules
- Responsible for the coordination of all alternate site disaster recovery efforts

2.2.3 IT Emergency Preparedness Committee Interface

- Interface with the EPC to ensure that an open line of communication is maintained throughout any incident where the IT Disaster Recovery Organization is active

2.2.4 Operations Manager

- Work alternating shifts with a transition overlap before and after each shift
- Brief the on-coming Operations Manager prior to assuming shift responsibilities on executed and pending planned activities
- Primary responsibilities:
  - Assume leadership of all activities on site throughout their shift
  - Escalate issues as needed or required
  - Coordinate all activities associated with Meals/Accommodations
  - Assure all staff are present or to call in support as needed
  - Manage the on call list and coordinate task with the IT Command Center Duty Manager
  - Update the dashboard on Web EX
  - Coordinate all activities scheduled and manage timeline
  - Manage Web EX on line for updates on issues/progress

2.2.5 Duty Manager

- Work alternating shifts with a transition overlap before and after each shift
- Brief the on-coming Duty Manager prior to assuming their shift responsibilities on executed and pending planned activities
- Interface with SunGard personnel at the computer recovery facility as the WellCare management representative
- Participate in the preparation of initial damage assessment report as appropriate.
- Update WellCare IT DR Recovery Executive or alternate as required on progress, problems, etc.
- Provide management and control of the event by:
  - Manage the call bridge
  - Manage the DR Dashboard
  - Hour by Hour management of the Command Center
  - Manage Contacts/Escalations
  - Manage the resource Plan
  - Manage an issues log and all issues pertaining to the recovery
  - Receive briefing from the IT DR Recovery Executive or alternate as appropriate and provide updates to the alternate site infrastructure recovery team leaders.
  - Work with Alternate site IT DR Team Leaders to evaluate recovery options and establish priority requirements.
  - Work with alternate site IT DR Team Leaders to develop personnel schedule to track WellCare alternate site staffing at all times.
  - Assess preparedness of alternate site infrastructure recovery teams to respond to the disaster; modify assignments and responsibilities as necessary.
  - Meet daily with alternate site IT DR Team Leaders who have personnel involved in recovery site work to be apprised of situation changes and changes in personnel support requirements.
  - Contact alternate site IT DR Team Leaders daily, to communicate needs and changes in status.
  - Update IT DR Recovery Executive as required on progress, problems, etc.

2.3 IT Recovery Infrastructure Support

These teams are responsible for documenting and maintaining the technical recovery procedures in addition to participating in recovery exercise and an actual disaster event. Some IT infrastructure recovery and support processes may function remote from the recovery data center or will be located at the IT Command Center.

The role of Logistics and Administration Support is assigned to a resource at time of crisis. The primary responsibility is to support the ITRM team lead by:

- Logging events and issues.
- Scheduling of status call and other meetings as required.
- Coordinating any travel, accommodations, transportation, meals and any other logistical needs as they arise.

2.4 EPC Support Functions

If required, EPC Support functions may operate from the IT Command Center when activated or from the Corporate Command Center through the Emergency Preparedness Committee (EPC). See the 2014 IT EPP.PR document for details.

3 Disaster Declaration

Disaster declaration is a formal decision by pre-authorized personnel that a disaster or severe outage is predicted or has occurred and that triggers pre-arranged mitigating actions (e.g., a move to an alternate site.)

Note: There are significant SunGard contractual fees ($1M +) associated with "declaring" a disaster the decision to declare cannot be taken lightly.

A disaster can be one of three ways, the obvious "smoking hole" where no assessment and justification is required to declare. Next is the less obvious where the disruption will take some time to assess and understand to determine if a declaration is warranted. Lastly is the imminent event such as a hurricane. In this case WellCare may choose to declare a disaster with SunGard by following the processes defined in Appendix 5.9 IT DR Preparation.

Declaring a disaster will result in invoking the recovery procedures in either the IT Business Recovery Plans and/or the IT Disaster Recovery Plans, depending on the event.

On-site management through the IT Disaster Recovery Executive is expected to "qualify" the disaster and recommend the level of plan escalation to be initiated. In order to make a realistic decision, the outage duration must be a realistic estimate and not an optimistic expectation.

Certain factors and/or criteria will affect the qualification process and must be weighed in making the disaster organization mobilization judgment. Some considerations may include the following:

1. Day of the week, month, or time of the year
2. Customer and provider requirements
3. Magnitude of event and confidence in estimated time to repair or replace.
4. Nature of threat, i.e., bomb scare or actual event.
5. Non-facility-related event, i.e., caused by widespread communications or power failure, earthquake, hurricane, tornado, toxic spill envelopment, etc.
6. Localized problem affecting only some areas of the facility.

3.1 Authority

The Emergency Preparedness Committee (EPC) has the final decision level in declaring a disaster and mobilizing the IT Disaster Recovery Organization. The decision is dependent upon a recommendation from the IT Disaster Recovery Executive, the ITRM Team Lead(s), other key personnel and all of the available information and the results from a damage assessment in determining the extent and impact of the interruption.

Disaster declaration is activated under the direction and authority of the WellCare Corporate Emergency Preparedness Committee (EPC) in cooperation with the WellCare Information Technology (IT) VP Infrastructure.

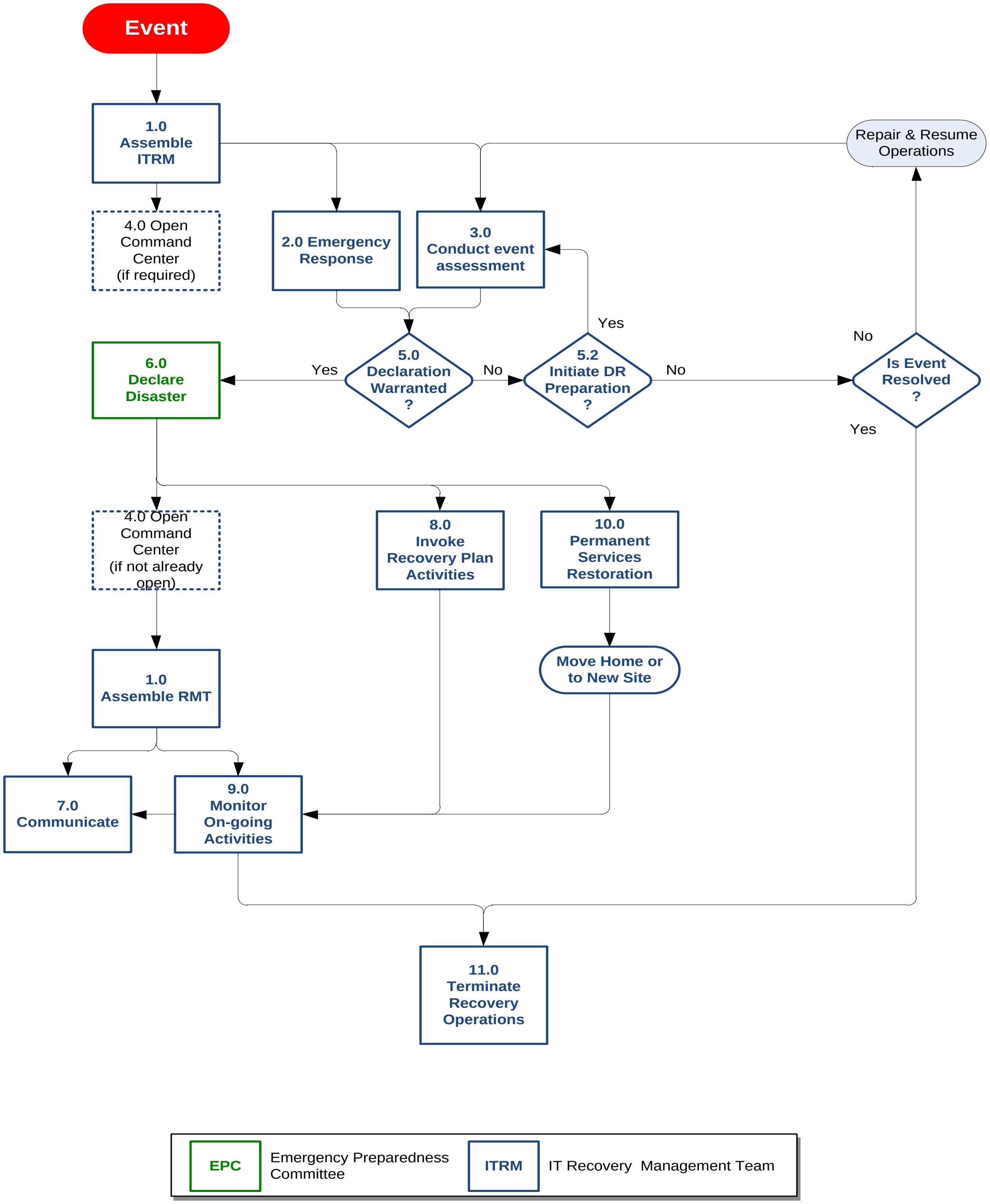
Once the EPC approves the recommendation from the CIO to declare, one of the leaders identified on the SunGard Disaster Declaration Authority List must call and declare a disaster.

- Call SunGard @ **(866) 722-1313**
- Whomever calls, must identify themselves as an Authorized Disaster Declaration Authority and provide the declaration authorization code to the SunGard representative
- Wellcare Customer ID 276187

3.2 SunGard Disaster Declaration Authority List

Name	Title
Darren Ghanayem	CIO, Operations
Paul Kohler	VP, IT Infrastructure
Lydia Ophaug	Director, IT-Client Services
Matthew Hubbard	Sr. Manager, Enterprise Proj Dev, IT Client Services
Wayne Harrison	Technical Project Manager, IT-Client Services

4 Disaster Operations


Event
1.0 Assemble ITRM
4.0 Open Command Center (if required)
2.0 Emergency Response
3.0 Conduct event assessment
Repair & Resume Operations
Yes
No
5.0 Declaration Warranted ?
5.2 Initiate DR Preparation ?
Is Event Resolved ?
Yes
No
No
Yes
6.0 Declare Disaster
4.0 Open Command Center (if not already open)
8.0 Invoke Recovery Plan Activities
10.0 Permanent Services Restoration
Move Home or to New Site
1.0 Assemble RMT
7.0 Communicate
9.0 Monitor On-going Activities
11.0 Terminate Recovery Operations
EPC
Emergency Preparedness Committee
ITRM
IT Recovery Management Team

4.1 ITRM Process Flow Checklist

Following notification of an incident affecting data center operations, the ITRM team may follow the process as outlined in the process flow checklist below. Details for the below table are found in section 4.2 ITRM Recovery Task List within this document.

Step	Action	Activity Summary
1.	Assemble the Decision Makers	After notification by the EPC or *other management* open a conference bridge ------------------------- **Audio Conference** ------------------------- **USA Toll-Free:** 844-531-9390 **USA Caller Paid/International Toll:** 669-234-1179 **ACCESS CODE:** 9192208 **HOST PASSWORD:** 91284674 --------------------------- **Web Meeting** --------------------------- Web meeting will be opened via Citrix WebEx
2.	Emergency Response	Initiate Evacuation Procedures if appropriate. Once staff is evacuated, assembled, and the leads have determined status; communicate information to the Emergency Preparedness Committee and/or Civil Authorities of any immediate issues or concerns.
3.	Assess the Situation Damage	Collect situation information: Status of employees / Site damage assessment / IT infrastructure / Data / IT Systems / site security Effects on customers / vendors
4.	Setup the IT virtual or physical Command Center if not accomplished in 1 above	------------------------- **Audio Conference** ------------------------- **USA Toll-Free:** 844-531-9390 **USA Caller Paid/International Toll:** 669-234-1179 **ACCESS CODE:** 9192208 **HOST PASSWORD:** 91284674 --------------------------- **Web Meeting** --------------------------- Web meeting will be opened via Citrix WebEx

Step	Action	Activity Summary
5.	Recovery Decision: Go / NO GO	Determine from 3.0 assessments if declaration is warranted or if more time is needed to resolve incident. If declaration is warranted, communicate to the CIO/EPC and request approval to declare. If a declaration is imminent then initiate the IT DR Preparation process. See Appendix 5.9 IT DR Preparation
6.	Declare Disaster	Declaration approval made by VP Infrastructure/EPC, IT Disaster Recovery Executive activates recovery teams
7.	Communication Information	Establish schedule for situation report status calls. Continue with upstream and downstream communications
8.	Invoke Recovery Plans	IT disaster recovery plan is activated by notification of recovery teams to begin with the tactical recovery effort.
9.	Monitor On-going Event Activities	Conduct status calls with all IT recovery teams and report progress to VP Infrastructure/EPC
10.	Permanent Services Restoration	Based on the situation assessment, determine if rebuild or repair can be performed or if a build out of a new facility is necessary. Begin planning for return to home activities.
11.	Terminate Recovery Operations	IT Disaster Recovery Executive, IT Alternate Site Executive and ITRM Team Lead determine demobilizing the ITS Command and Control and termination of recovery operations

4.2 ITRM Recovery Task List

If there is an obvious disaster go directly to Step 6.0 Declare the Disaster

If not, follow Steps 1.0 Assemble the decision-makers through 5.0 Recovery Decision

Step #	Task	Responsibility
1.0	**Phase 0: Incident Identification - Assemble the decision-makers**	
1.1	Initial notification of an event: Did the information come from the CIO or EPC and if not, is the VP Infrastructure/EPC aware of the situation? Inform the CIO/EPC if appropriate. Does the event warrant an immediate declaration? If yes, proceed to 1.3. If no, proceed to 1.2	IT Disaster Recovery Executive
1.2	Engage the IT Recovery Management team (ITRM). Any member of the ITRM can convene the ITRM. If required, engage in IT Disaster Recovery Virtual Command Center meetings on the half hour at: -------------------------- **Audio Conference** -------------------------- **USA Toll-Free:** 844-531-9390 **USA Caller Paid/International Toll:** 669-234-1179 **ACCESS CODE:** 9192208 **HOST PASSWORD:** 91284674 ---------------------------- **Web Meeting** ---------------------------- Web meeting will be opened via Citrix WebEx If an outbound line is not available, communicate with others using a mobile telephone.	IT Disaster Recovery Executive ITRM Team Lead

	If required, engage in IT Virtual Command Center meetings on the half hour at: -------------------------- Audio Conference -------------------------- **USA Toll-Free:** 844-531-9390 **USA Caller Paid/International Toll:** 669-234-1179 **ACCESS CODE:** 9192208 **HOST PASSWORD:** 91284674 ---------------------------- Web Meeting ---------------------------- Web meeting will be opened via Citrix WebEx If an outbound line is not available, communicate with others using a mobile telephone. If the incident affects the safety of WellCare employees, immediately activate Step 2.0 Emergency Response. If a disaster declaration has occurred, immediately activate, Step 6.0 IT Disaster Declaration. If further incident assessment is required, activate Step 3.0 Incident Assessment.	IT Disaster Recovery Executive ITRM Team Lead

Step #	Task	Responsibility
2.0	**Emergency Response**	
2.1	Execute the **Emergency Response** as detailed in the remainder of this phase. This plan applies to all departments that have staff located at the affected site. IT departments considered to be **critical** and their individual **Recovery Time Objectives** are as follows: IT Infrastructure Services (Tier 0 - 24 hours)	IT Disaster Recovery Executive ITRM Team Lead
2.2	Immediate Response to Business Disruption The immediate response to any significant event includes building evacuation, staff assembly, staff head count and notification of off-site staff. **1. Initiate Evacuation Procedures, if appropriate**, in accordance with all fire and safety procedures. All staff will be directed to assemble outside of the building at each employee’s Evacuation Assembly Point; this is pre-determined by the work location of each person. Staff will report to their manager to ensure they are accounted for. Staff will remain in the assembly area until the Police or Fire Department, or IT management issues further orders. **2. Determine if all personnel have evacuated.** Managers will determine if all personnel have evacuated. Communicate any staff issues and/or concerns to the senior manager present and/or civil authorities.	IT Disaster Recovery Executive ITRM Team Lead

Step #	Task	Responsibility
2.3	Alert Managers and Critical Staff When staff are evacuated, assembled, and the leads have determined status; communicate information to the Emergency Preparedness Committee and/or Civil Authorities of any immediate issues or concerns. If required, engage in IT Virtual Command Center meetings **on the half hour** at -------------------------- **Audio Conference** -------------------------- **USA Toll-Free:** 844-531-9390 **USA Caller Paid/International Toll:** 669-234-1179 **ACCESS CODE:** 9192208 **HOST PASSWORD:** 91284674 ---------------------------- **Web Meeting** ---------------------------- Web meeting will be opened via Citrix WebEx If an outbound line is not available, communicate with others using a mobile telephone as an alternative communications solution. Await further direction from the Emergency Preparedness Committee or CIO. As directed, execute the IT Disaster Recovery Plan.	IT Disaster Recovery Executive ITRM Team Lead
3.0	**Incident Assessment - Assess the situation/damage**	
3.1.	Determine and verify the severity of the incident and the current status. If necessary, arrange a site visit by coordinating with building manager, building security and local authorities. Communicate the severity and the current status of the incident during scheduled IT Virtual Command Center conference calls.	IT Disaster Recovery Executive ITRM Team Lead

Step #	Task	Responsibility
3.2.	If data center damage assessment is required, ensure that sufficient knowledgeable personnel are available to adequately appraise equipment and network damage and equipment salvage potential.	IT Disaster Recovery Executive ITRM Team Lead
3.3.	Provide ongoing updates regarding impact on technology infrastructure to the Emergency Preparedness Committee during scheduled conference calls. Provide recommendations regarding disaster declaration.	IT Disaster Recovery Executive IT Emergency Preparedness Committee Interface
3.4.	Alert key vendors of the situation, advise them that their services may be needed and ask them to await further instructions.	ITS Recovery Team Leaders
3.5.	If the incident is a disaster, activate Step 6.0 IT Disaster Declaration. If the incident is a disaster, activate Step 4.0 Activate IT Disaster Recovery Command Center. If the incident is external to the data center and the data center site has not been damaged, decide whether a formal declaration can be deferred pending resolution of the incident. See next step 3.5 If a Damage Assessment is required, go to step 3.8, Conduct Damage Assessment. If the Emergency Preparedness Committee has clearly communicated that the incident is not a disaster, terminate the IT Disaster Recovery Plan execution. Otherwise, continue to analyze and monitor the incident, provide updates to the Emergency Preparedness Committee and confirm incident status.	IT Disaster Recovery Executive
3.6.	**Co-location site Evacuation**: Determine whether the IT infrastructure can be allowed to operate for some time before further consideration of a disaster declaration is required. Some factors to consider in making this decision are: The nature of the incident. For example, a railway or trucking accident could release fumes or smoke that could get drawn into the air in-take ducts and could contaminate the data center, a regional power outage with an undetermined power restoration time frame, civil unrest, etc.	IT Disaster Recovery Executive
3.7.	Develop damage assessment strategy, assign resources from available resources identified in 3.2 and instruct the selected team to conduct IT Damage Assessment. If an outbound line is not available, communicate with others using a mobile telephone.	IT Disaster Recovery Executive ITRM Team Lead

Step #	Task	Responsibility
3.8.	**Conduct Damage Assessment:** Prepare a complete damage assessment log/inventory of all damage and the repairs required to restore affected technology infrastructure to original condition. See Appendix for forms. If required, conduct site visits to further assess damage. Coordinate with site security, facility operator and local authorities to arrange the visit. Report damage assessments to IT Disaster Recovery Executive and Emergency Preparedness Committee or other corporate management as instructed.	ITRM Team Lead
3.9.	Review input from the ITRM damage assessment: estimate the total damage and probable duration of the outage.	IT Disaster Recovery Executive ITRM Team Lead
3.10.	Facilitate damage assessment meetings, including a comprehensive briefing on the status of: Affected facilities, equipment, systems and services. Accessibility to affected WellCare buildings and equipment. Scope of damage/outage (local, regional, national, international	IT Disaster Recovery Executive ITRM Team Lead
3.11.	Utilize damage assessment to assist appropriate corporate departments to substantiate insurance claims.	ITRM Team Lead

Step #	Task	Responsibility
3.12.	Engage other members of the corporate recovery organization (Facilities, Real Estate, IT, Engineering) for the following additional services as required: • Restoration from Fire and Water Damage • Desiccant Dehumidification • Electronics Recovery • Debris Removal • HVAC Decontamination • Mold Remediation • Environmental Remediation Regulatory Compliance • Salvage Appraisals • Building Reconstruction	ITRM Team Lead
3.13.	Via scheduled conference calls, notify the ITRM team and the CIO/EPC of the damage estimates and probable outage duration.	ITRM Team Lead
3.14.	Proceed with one of the following options: • Step 5.0 Recovery Decision Go/No-go • Continue to monitor the incident • Terminate Recovery activities	IT Disaster Recovery Executive ITRM Team Lead

Step #	Task	Responsibility
4.0	**Activate IT Disaster Recovery Command Center**	
4.1.	The IT Disaster Recovery Command Center is first established as a virtual meeting place by using the below information. The Virtual IT Command Center is activated Step 1.0 – 1.2 in this document. If the situation warrants, the ITRM team will assemble in a TBD office location and if unavailable, the team will utilize the virtual Command Center as the primary: -------------------------- **Audio Conference** -------------------------- **USA Toll-Free:** 844-531-9390 **USA Caller Paid/International Toll:** 669-234-1179 **ACCESS CODE:** 9192208 **HOST PASSWORD:** 91284674 ---------------------------- **Web Meeting** ---------------------------- Web meeting will be opened via Citrix WebEx If an outbound line is not available, communicate with others using a mobile telephone. **IT Disaster Recovery Command Center:** SunGard work area recovery center-Primary Site 300 Primera Blvd., Suite 308 Lake Mary, FL. 407.833.4440 SunGard work area recovery center-Secondary Site 1055 Spring St. NW, Atlanta, GA 30309 404-448-2531	IT Disaster Recovery Executive ITRM Team Lead

Step #	Task	Responsibility
4.2.	The following must be done to activate the TBD office location when being used as the IT Disaster Recovery Command Center: • Validate Internet access • Validate phones are operational o Individual & speakers o POTS lines (incoming only & outgoing only) • Fax • Copier (paper & toner) • Radio/TV • PC w/ projector (printer w/ paper & toner) • Flip charts and/or whiteboard and markers • Overhead projectors • Recovery Plans • Multiple copies of any log sheets to be used in the Command Center (call logs & Action Plan, for example) • Notebooks/paper/pens	IT Disaster Recovery Executive ITRM Team Lead
4.3.	Contact Hotel to secure meeting room Hotel Contact: TBD- depends on location PM will have this information Number: enter TBD-depends on location PM will have this information Room requirements: • No of seats • Speaker phone • White board/markers • Easel/flip charts/markers	ITRM Team Lead
5.0	**Declaration Decision – GO / NO GO**	
5.1.	Convene the IT Recovery Management Team as follows: Customize the message: ‘Please call the ITS Disaster Declaration Team bridge line at:	IT Disaster Recovery Executive ITRM Team Lead

Step #	Task	Responsibility
	-------------------------- **Audio Conference** -------------------------- **USA Toll-Free:** 844-531-9390 **USA Caller Paid/International Toll:** 669-234-1179 **ACCESS CODE:** 9192208 **HOST PASSWORD:** 91284674 ---------------------------- **Web Meeting** ---------------------------- Web meeting will be opened via Citrix WebEx (This bridge may have been established previously, but if not convene at this time.) To access the names and telephone numbers see Appendix A - ITRM team contact list.	
5.2.	If ITRM decides to recommend a declaration of an IT disaster, request authorization from the CIO/EPC. Provide instructions regarding planning/preparation activities. ***If a disaster in imminent but not immediate, initiate IT DR Preparation processes. See Appendix 5.9.***	IT Disaster Recovery Executive ITRM Team Lead
5.3.	If VP Infrastructure or EPC authorizes the declaration, proceed with Section 6.0 IT Disaster Declaration	IT Disaster Recovery Executive ITRM Team Lead
6.0	**IT Disaster Declaration**	
6.1.	If the decision to declare was obvious and if not already done so, follow the tasks in 1.0 Assemble the Decision Makers and 4.0 Setup the IT virtual or physical Command Center To register a declaration or alert with SunGard call: Call SunGard @ (866) 722-1313 Whomever calls, must identify themselves as an Authorized Disaster Declaration Authority and provide the declaration authorization code to the SunGard representative	IT Disaster Recovery Executive ITRM Team Lead

Step #	Task	Responsibility
	Remind SunGard that information regarding the disaster event, including SunGard involvement in its resolution, is considered to be strictly confidential.	
6.2.	Alert other key vendors that need to be made aware of the IT Disaster Declaration.	ITRM Team Lead
6.3.	Notify business unit managers.	ITRM Team Lead
6.4.	Once the IT Disaster Declaration has occurred, convene the ITRM to issue initial instructions, priority changes, plans, etc. for executing the IT disaster recovery plan.	IT Disaster Recovery Executive ITRM Team Lead IT Disaster Recovery Team Leaders
6.5.	Activate, Section 7.0 Recovery Team Response.	IT Disaster Recovery Executive
7.0	**DR Recovery Team Response - Invoke IT DR Plans**	
7.1.	Instruct the ITRM Team Lead to activate the IT disaster recovery plan to begin mobilizing resources (Step 7.2).	IT Disaster Recovery Executive

Step #	Task	Responsibility
7.2.	Each DR team will mobilize its resources with instructions to engage in a teleconference call. Customize the following message that will be sent to your recovery team: ‘Please call the Recovery Team bridge line at: ------------------------- **Audio Conference** ------------------------- **USA Toll-Free:** 844-531-9390 **USA Caller Paid/International Toll:** 669-234-1179 **ACCESS CODE:** 9192208 **HOST PASSWORD:** 91284674 --------------------------- **Web Meeting** --------------------------- Web meeting will be opened via Citrix WebEx Conduct the ITRM conference call using the selected bridge line and informs teams begin the recovery process.	ITRM Team Lead
7.3.	Notifications: Present External Web-page message Internal/External communications as documented	Emergency Preparedness Committee
7.4.	Mobilize Away-Team Identify available Away-Team members Schedule travel & accommodations	ITRM Team Lead IT Disaster Recovery Team Leaders
7.5.	Tape Validation: Identify any critical backup tape ids required Ship onsite tapes to SunGard Ship tapes from archive vendor(Iron mountain) to SunGard	IT Disaster Recovery Team Leaders

Step #	Task	Responsibility
7.6.	Away-Teams: Inventory received tapes at SunGard Validate WellCare equipment on site at SunGard Validate SunGard supplied recovery equipment	IT Disaster Recovery Team Leaders
7.7.	Initiate Infrastructure Recovery Processes at computer recovery facility Provide a list of infrastructure plans and the sequence diagram to enable progress monitoring	IT Disaster Recovery Executive ITRM Team Lead IT Disaster Recovery Team Leaders
8.0	**Monitor On-going Event Activities**	
8.1.	Schedule and conduct Team Leader status calls to obtain update for the CIO/EPC Customize the following message that will be sent to your recovery team: ‘Please call the Recovery Team bridge line at: -------------------------- **Audio Conference** -------------------------- **USA Toll-Free:** 844-531-9390 **USA Caller Paid/International Toll:** 669-234-1179 **ACCESS CODE:** 9192208 **HOST PASSWORD:** 91284674 ---------------------------- **Web Meeting** ---------------------------- Web meeting will be opened via Citrix WebEx	IT Disaster Recovery Executive ITRM Team Lead IT Disaster Recovery Team Leaders
8.2.	Report status to CIO/EPC	IT Disaster Recovery Executive IT Emergency Preparedness Committee Interface
8.3.	Report status to executive management	CIO

Step #	Task	Responsibility
9.0	**Permanent Services Restoration**	
9.1.	Decide to remain at hot-sites or rebuild/repair primary data center.	EPC CIO IT Disaster Recovery Executive
9.2.	Rebuild: Complete damage assessment activities. Provide assessment and recommendation to the Emergency Preparedness Committee through the IT Disaster Recovery Executive. Recommend required facility upgrades to Corporate Real Estate, Facilities & Engineering, and Architects. Order equipment and arrange to repair restorable IT devices. Install, make operational and test new equipment. Prepare to move operations. Move operations from SunGard to restored data center. Assist the Emergency Preparedness Committee with collection of documentation for insurance and reporting.	IT Disaster Recovery Executive ITRM Team Lead IT Disaster Recovery Team Leaders
9.3.	Build New Facility: Complete damage assessment activities. Provide assessment and recommendation to the Emergency Preparedness Committee. Design new data center specifications for Corporate Real Estate, Facilities & Engineering, and Architects. Order equipment for the new data center upon design approval. Install, make operational, and test new IT equipment in the newly built facility. Prepare to move operations. Move operations from Recovery Site to the new data processing facility Assist the Emergency Preparedness Committee with collection of documentation for insurance and reporting. Submit recommendations for return to normal services at the permanent data center location.	IT Disaster Recovery Executive ITRM Team Lead IT Disaster Recovery Team Leaders

Step #	Task	Responsibility
9.4.	Return: Lead a planned return to normal operating conditions at the permanent data center location. Conduct major data transfer to the permanent data center with full daily production ramp-up. Migrate data to permanent facilities. Complete permanent restoration of all services to the permanent data center facility. Approve restoration of full production capability to original service levels.	IT Disaster Recovery Executive ITRM Team Lead IT Disaster Recovery Team Leaders
9.5.	Activate Step 10 Terminate Recovery Operations	IT Disaster Recovery Executive
10.0	**Terminate Recovery Operations**	
10.1.	When all systems, operations and services have returned to normal operating mode, perform the following activities and tasks: Execute disposal of damaged equipment and materials. Analyze the results of the Recovery process to identify any errors, omissions or areas where improvements are required. Perform financial reconciliation and costs analysis. Conduct post incident review with all team leaders. Conduct internal and/or external audits of the Recovery process to determine the effectiveness of IT Disaster Recovery Plan. Identify critical initiatives, submit proposals and seek approval for implementation. Upgrade and/or update the IT Disaster Recovery Plan to incorporate required improvements. Identify improvements required to the staff training programs and plan training sessions to cover these areas.	IT Disaster Recovery Executive

5 Appendix

5.1 IT Recovery Management Team Contact List

ITRM Team	Leader	Alternate
CIO	Darren Ghanayem • Work: 813-206-7059 • Mobile: • Darren.ghanayem@wellcare.com Can Declare with SunGard	
IT Disaster Recovery Executive	Paul Kohler • Work: 813-206-2155 • Mobile: 813-373-1672 • Paul.Kohler@wellcare.com Can Declare with SunGard	John Rhome • Work: 813-206-7209 Mobile: 813-346-8794 • John.Rhome@wellcare.com
ITRM Team Lead (Alternate Site)	Jim Harrison • Work: 813-206-5730 • Mobile: 813-391-4763 Jim.Harrison@wellcare.com	Michael Lawley • Work: 813-206-1964 • Mobile: 813-476-4769 Michael.Lowley@wellcare.com
ITRM Team Lead	Wayne Harrisonard • Work: 813-206-6040 • Mobile: 813-846-4944 • Matthew.Hubbard@WellCare.com Can Declare with SunGard	Kathy Gracia • Work: 813-206-4566 Mobile: 813-601-9139 • Kathy.Gracia@wellcare.com
IT Disaster Recovery Command Center Duty Manager	Lydia Ophaug • Work: 813-206-5957 • Mobile: 813-833-7399 • Lydia.Ophaug@wellcare.com Can Declare with SunGard	Matt Hubbard • Work: 813-206-6064 • Mobile: 813-316-8184 Matthey.Hubbard@wellcre.com
IT Disaster Recovery Alternate Site Duty Manager	Jim Harrison • Work: 813-206-5730 • Mobile: 813-391-4763 • Jim.Harrison@wellcare.com	Greg Longo • Work: 813-206-3541 Mobile: 352-238-4694 Gregory.Longo@wellcare.com
IT Disaster Recovery Command Center Operations Manager	Wayne Harrison • Work: 813-206-6771 • Mobile : 863-512-1600 • Wayne.Harrison@wellcare.com Can Declare with SunGard	Matthew Hubbard • Work: 813-206-6040 • Mobile: 813-846-4944 • Matthew.Hubbard@WellCare.com Can Declare with SunGard
IT Infrastructure Windows and VMWare Team Lead	• Neal Gawthrop • Work: 813-206-7470 • Mobile: 727-753-8686 • Neal.Gawthrop@wellcare.com	Juan Calvo • Work: 813-206-7288 • Mobile: 813-767-8110 • Antonio.Braxton@wellcare.com
IT Infrastructure UNIX Team Lead	Rob Blayet • Work : 813-206-1641 • Mobile : 813-205-1565 • Robert.Blayet@wellcare.com	Chris Fenton • Work : 813-206-1305 • Mobile : 727-742-6325 • Chris.fenton@wellcare.com

ITRM Team	Leader	Alternate
IT Infrastructure Storage Team Lead	Carlos Velasco • Work: 813-206-7473 • Mobile: 813-340-7524 • Carlos.Velasco1@wellcare.com	Chris Neuner • Work:813-206-2604 • Mobile: 813-317-7385 • **Christopher.Neuner@wellcare.con**
IT Infrastructure Network Team Lead	Israel Rodriguez • Work: 813-206-5083 • Mobile: 813-307-0107 • Israel.Rodriguez@wellcare.com	Rhandy Figueroa • Work: 813-206-5413 • Mobile: 813-503-6959 • Rhandy.Figueroa@wellcare.com
IT Infrastructure Network Telephony Team Lead	David Valerius • Work: 813-206-1235 • Mobile: 813-363-5426 • David.Valerius@wellcare.com	Mickey Francisco • Work: 813-206-2804 • Mobile: 813-382-7883 • Roy.Wise@wellcare.com
IT Infrastructure Database Administration Team Lead	Prasad Kodali - Oracle • Work: 813-206-6770 • Mobile: 813-382-3222 • Prasad.Kodali@wellcare.com	Pavan Posani - My SQL • Work: 813-206-5821 • Mobile: 813-215-7840 • Praveen.Reddy@wellcare.com
EPC Representative	Danielle Miller • Work: 813-206-4556 • Mobile: 727-709-7989 Danielle.Hancock@wellcare.com	
Name	**Role**	**Contact #**
Chris Thomas	Alfresco	813-996-6751
Peter Farrell	Autosys	813-362-7812
Frank Polino		813-508-0889
John Dossou	Care Connects	813-476-5687
Prince Antony		614-329-9935
Yury Brei		727-902-0297
Didi Flechas	Check Run	813-625-3448
Amhed Suarez	CIS	786-308-7792
Clint Barnett		813-240-6392
Sachin Shah	CES	727-831-4852
Pradhdeep Singh	CPR+	716408-4950
Lakhan Melugiri		
Chris Thomas	Documentum - Customer Service	813-996-6751
Claudia Poo enciso	E2F	813-789-8092
Lei Luo		
Ashutosh Sood		813-739-9425
Craig Smitman	EDI	941-704-1539
Mohan Patha		337-412-8264
Anson Tharakunnel	EMMA	561-901-3035

ITRM Team	Leader	Alternate
Prabhdeep Singh		716-408-4950
Lakhan Melugiri		407-233-6230
Matt Ayres	Encounters	
Matt Cohen	ESB/Jboss	813-400-9828
Kat Schroeder	FCS (cts,vdp,cds,eob,res)	813-841-1267
Victor Gonzalez	CTS (Correspondence Tracking System)	787-378-0204
	CDS (Correspondence Delivery System)	
	VDP (Variable Data Publishing)	
Pramod Reddy	HIP	813-340-4580
Merline Sigamini		813-753-9299
Eric Gledhill		941-725-0119
Larry Holden	Informatica	813-304-5349
Avinash Vintha		571-527-8217
Alexandra D'Agata	MoveIt	813-368-0362
Jim Roberts		727-560-4611
Susan Keyser		904-422-2561
Kondaiah Swarna	MQ	
Ravi Ainpudi	Oracle Financials	813-390-9929
Sujatha Inampudi		813-395-4557
Bhanu Thatikonda	Pega MMP/UM/PHM	954-328-7022
Ratan Kumar		954-516-3294
Promil Pandey	Pega CarePath	
Ann Shanthakumar		
Cody Pagunsan	Pega EWF	321-287-6223
Chris Keating	Pega CLAIMS PATH	352-223-2438
Fabian Diaz	Pega Administration	
Jonathan Elrom	RightFax	727-798-2019
Chandra Mogulla		845-389-7965
Kristy Triantafilu	Sailpoint	727-439-5835
Racquel Reid		813-409-7228
(Internal testing)	SAS	571-527-8217
Jason De La torre	Sharepoint	813-774-2827
Susan Brower		
Kosty Surkov	SSO	727-688-9291

ITRM Team	Leader	Alternate
	Subversion	
Pramod Reddy	TFS	813-340-4580
Eric Gledhill		941-725-0119
Warren Goldstein	WC Toolbox (Appeals & Grievances	727-421-2401
Praveen Krishna	Web (WC.COM)	
Giridhar Phaneendra		
Kartik Boreda	Webservices	408-506-9453
Smitha Ramesh		813-464-5208
Kumaran Subramanian	Xcelys	81`3-459-4861
Sudhir Hirode		813-317-8274

IT Disaster Recovery Status Call

Status calls are recommended to be at least every half hour with executive updates on a periodic basis.

Status Call Agenda:

Situation	What is the current status?
Incident Action Plan	What are the priorities and objectives for the current time period?
Organization & Assignments	Who is involved? Where are they? What are they doing?
Resources	What resources are needed, by whom and when? What is the stat of resources requested but not available yet? What resources will be needed in the future (e.g., people, equipment, funds)
Communications	What will be the messages to internal and external stakeholders? Set the date and time for the next Checkpoint Call.
Parking Lot	Issues that have been identified for later resolution
Determine actions that need to occur before the next Checkpoint call (called an Operational Period)	Document the actions on the Incident Action Plan form. The source file is located at:

5.2 Incident Action Plan Form

Incident:

Item #	Item	Pri.	Resp.	Opened	Last Updated	Closed	Target Close	Comments/Status

The purpose of the Incident Action Plan form is to document what the activity priorities are for each "Operational Period" (the time between each checkpoint call). Based on information obtained during each checkpoint call, the Disaster Recovery Incident Manager will approve the priorities of activities for the next Operational Period. The administration support will then document those priorities on the Exercise Completion Checklist and post in the IT Command Center as well as distribute to the appropriate stakeholders

5.3 Command Center Issues Log

An issue log will be maintained for each issue encountered during the exercise and will be incorporated into the Post Exercise reporting.

Issue #	Date	Issue	Issue Type	Identified By:	Resolution Type	Resolution	Resolved By	Action	Impact if not resolved	Assigned To	Date Closed

5.4 Added Expense Checklist

This is provided as a tool to finance to assist in determining the expenses that are incurred specifically because of a long-term disrupting event. This information is necessary in determining potential insurance claims to WellCare's insurance provider. Any potential insurance coverage will depend on WellCare-specific policies.

GUIDE TO DETERMINE AMOUNT OF INCREASED COSTS INSURANCE REQUIRED

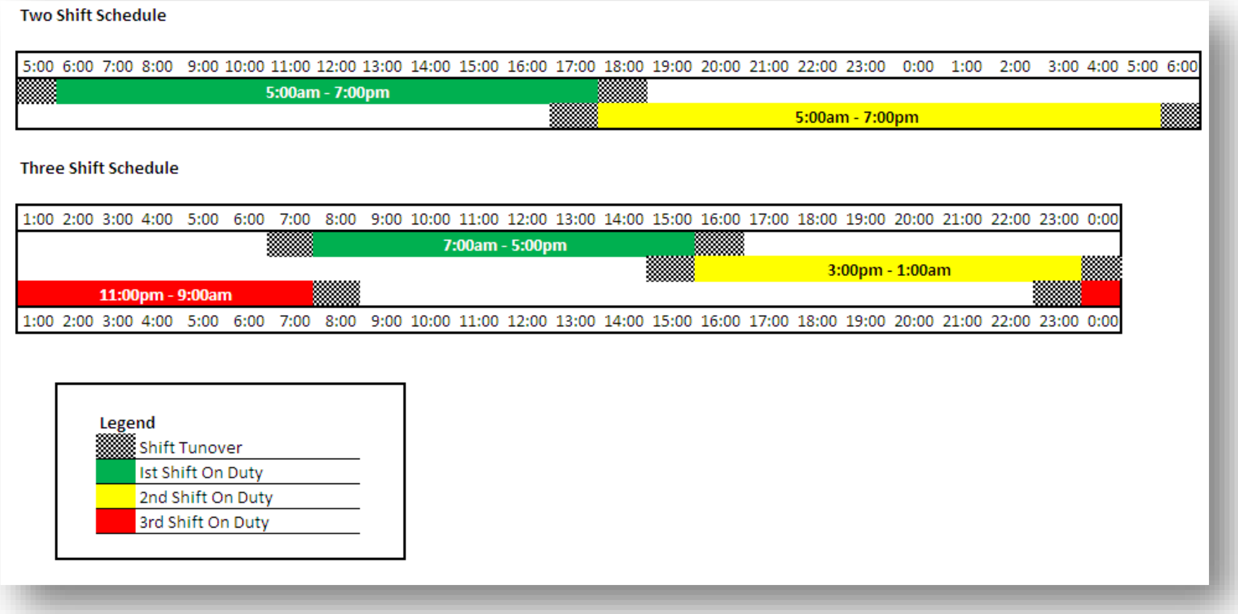
		1st Month $	2nd Month $	3rd Month $	Period Beyond 3 Months $
		(or an all-up estimate can be made)			
a.	Rental of temporary premises				
b.	Rental of temporary equipment or outsourcing				
c.	Uninsured cost of equipment purchased				
d.	Expense of moving equipment, etc.				
e.	Cost of cleaning temporary premises				
f.	Light, power, heat at temporary location				
g.	Telephone, email and IT installation at temporary location				
h.	Extra telephone and email cost				
i.	Special announcements in newspapers, on TV, or other crisis communication costs				
j.	Security protection service				
k.	Cost of engineering service or accommodation				
l.	Extra cost for transporting employees				
m.	Rental and use of cars/vehicles				
n.	Special bonuses and overtime to employees				
o.	Expenses of making arrangements to have supplies and raw materials delivered to another location				
p.	Differentials in freight rates due to different shipping points or airports				

q.	**TOTAL EXTRA EXPENSE**	____________	____________	____________	____________
r.	Deduct expenses discontinued at original locations because of loss	____________	____________	____________	____________
s.	**NET EXTRA EXPENSE TO INSURE**	____________	____________	____________	____________

5.5 IT Command Center Schedule

The IT Command Center Schedule will be established by the ITRM Team Leader, based on the needs of the situation and the resources available.

Below are examples of a two-shift schedule and a three-shift schedule format used by the Command Center. The ITRM Team Leader will make the decision of which schedule to use when the Command Center is activated. As the event continues, the ITRM Team Leader may choose to alter the schedule to the other format, based on the needs of the particular event.



Two Shift Schedule

5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00	0:00	1:00	2:00	3:00	4:00	5:00	6:00
▨	🟩 5:00am - 7:00pm	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	▨												
												▨	🟨 5:00am - 7:00pm	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	▨

Three Shift Schedule

1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00	0:00
						▨	🟩 7:00am - 5:00pm	🟩	🟩	🟩	🟩	🟩	🟩	🟩	▨								
														▨	🟨 3:00pm - 1:00am	🟨	🟨	🟨	🟨	🟨	🟨	🟨	▨
🟥 11:00pm - 9:00am	🟥	🟥	🟥	🟥	🟥	🟥	▨															▨	🟥
1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00	0:00

Legend

▨	Shift Tunover
🟩	Ist Shift On Duty
🟨	2nd Shift On Duty
🟥	3rd Shift On Duty

5.6 IT Command Center Locations

IT Command Center	Building/Address	Room	Direct Numbers
Primary	SunGard Recovery Center 300 Primera Blvd. Lake Mary, FL	Suite 308	(407) 833-4440
Secondary	Sungard Recovery Center 5600 United Drive Smyrna, GA 30082		(770) 434-9988

5.7 Communications – External Relations

External The EPC Corporate Communications staff will serve as media spokespersons for all WellCare sites. No other employees, contractors, WellCare partners or agents shall speak to the media about WellCare matters unless first cleared by the EPC Corporate Communications staff. (If the Corporate Communications support function of the EPC is not activated, then the IT DR Command Center may create an ad-hoc support function and team from Corporate Communications personnel.)

If and when you are contacted by the media in regard to any incident or story, please refer the reporter to Corporate Communications personnel or previously-designated spokespersons as soon as possible. Also, if possible, please obtain the name of the news organization, and the contact information of the reporter. As soon as possible, please let Corporate Communications know you were contacted and by whom.

In the event something occurs at the recovery facility or Command Center which has the potential of becoming a media story, please contact a member of the Corporate Communications staff *as soon as possible, regardless of the day or time, in addition to your manager*. If Corporate Communications cannot be reached, let your manager or supervisor know.

Let the Corporate Communications department and your manager know as soon as possible if you observe a member of the media arrive at the Command Center. The news media have a legal right to observe, photograph and record any event or any person on public property, so please do not attempt to interfere with that right. However, the Command Center and its parking lots are not public places; it is private property.

5.8 IT DR Preparation

Where possible, in advance of a high impact event, WellCare Information Technology will execute against the following disaster response time-line.

Disaster Event Phases:

Event Phase	Time-line	Activities	Owner
Event Alert	5 days	• Issue Event Alert • Alert DR Vendor (SunGard) • Identify / Secure Critical Tape Backup	• IT Infrastructure Mgmt.
Event Watch	T0 (-) 4 days	• Issue Event Watch • Ship Recovery Media • Declare Disaster w/SunGard • IT Team Travels to SunGard	• Corporate Executive • IT Leadership • IT Away Team
Event Warning	T0 (-) 24 hours	• Issue Event Warning • Activate Emergency Mode of Operations	• IT Leadership
DR Cut-Over Decision	T0 (+) 16 hours	• EPC decision to cut-over to SunGard • If 'no' continue operations • If 'yes', cut-over to SunGard • Execute IT Emergency Mode of Operations	• EPC / IT CIO

5.8.1 Event Alert Procedures

Event Watch procedures are activated approximately 72 hours prior to event impact

The following procedures are initiated at the discretion of the ITRM team based on event information from a recognized, official source; i.e., FEMA, National Weather Center, and local stations.

5.8.1.1 Issue Event Alert

The ITRM team will deem when it is necessary and will Issue an Event Alert to all IT Managers and above by any and all means of communications to include Emails, Outlook Calendar, SMS, and Voice.

5.8.1.2 Alert DR Vendor (SunGard)

The IT Infrastructure Management will notify SunGard at the below of an Alert Status;

SunGard Phone:	**(866) 722-1313**
Customer Name:	**AT&T Services, Inc.** (For Comprehensive Health Plans)
Customer Id:	**276187**

5.8.1.3 Identify and Secure Critical Tape Backup

The ITRM team will execute the following procedures:

1. Identify DR Recovery Backup Media
    a. Identify all physical tape IDs for the last three (3) full critical and production backups.
    b. Collect and prep all identified tapes that have not been forwarded to the tape archive.
    c. Create list of critical backup media that is located at the tape vendor's location.

Note: Data Domain and SRDF serve as the primary technology solutions for recovery. Tapes serve as a backup technology solution in the event of unforeseen issues with the primary technology solutions.

5.8.2 Event Watch Milestone Procedures

Event Watch procedures are activated approximately 48 hours prior to event impact.

The following procedures are initiated per the authority of the Corporate Emergency Preparedness Committee and the Information Technology Chief Information Officer (CIO) or delegate(s).

5.8.2.1 Ship Recovery Media

The ITRM team will manage the Wellcare contact (Bret Custer 813-505-7644) to the Tape Archive Vendor (Iron Mountain 813-644-4522-customer number 122972) to initiate shipment of backup media identified in section 5.8.1.3 of this document.

SunGard Tape Receiving Address:

SunGard Availability Services, LLC

777 Central Blvd.

Carlstadt, NJ 07072

(201) 729-2450

5.8.2.2 IT DR Away Team Travel Procedure

The ITRM team will designate the IT Away Team from availability of staff and skill set needed. The IT Away Team travels under the direction and authorization of the CIO and EPC and will adhere to WellCare's Internal Travel Policies and Procedures.

5.8.3 Disaster Recovery Declaration

The disaster recovery declaration with the remote recovery vendor is executed per the direction of the EPC and IT CIO. Refer to section 3.2 for a listing of IT leaders who are authorized to declare a disaster with the remote recovery vendor (currently SunGard).

One of the identified leaders must call and declare a disaster with the remote recovery vendor:

- Call SunGard @ **(866) 722-1313** Wellcare Customer ID 276187
- ➢ Whomever calls, must identify themselves as an Authorized Disaster Declaration Authority

5.8.4 Event Warning Milestone Procedures

Event Warning procedures are activated 24 hours in advance of Event impact.

The following procedures are initiated per the authority of the Corporate Emergency Preparedness Committee and the Information Technology Chief Information Officer (CIO) or delegate(s).

5.8.4.1 Event Warning Notification Procedure

ITRM team will notify all IT Managers and above that an Event Warning has been initiated by any and all means of communications to include Emails, Outlook Calendar, SMS, Voice and ENS system.

6 IT DISASTER RECOVERY PROCEDURES

The IT DR Incident Management Team will be accountable for execution of the recovery and the reporting to the CIO and Corporate Emergency Preparedness committee statuses and issues pertaining to the recovery.

6.1 Remote Data Center Recovery Procedures

All detailed recovery procedures are stored electronically on the SunGard Recovery Portal at https://www.sungardas.com The following will be recovered in the following order:

1. Validate Network
2. Configure DR Host Servers
3. Configure / Allocate DR Storage (SAN/NAS)
4. Establish Remote DR Citrix Farm
5. Fail over to DR Exchange Server
6. Verify DR Backup Domain
7. Restore Critical System Back-up Images
8. Recover and Verify Critical Applications

6.2 Applications Recovery Sequence

WellCare systems are recovered in the following order by the Recovery Time Objective (RTO) and the RPO as mandated by the Business in the annual Business Impact Assessments (BIA). Refer to the Appendix for the Mission Critical Applications referenced in the BIA’s.

- Tier 1 – RTO ≤ 12 Hrs. RPO ≤ 60 Min
  - Critical business interactions with members and providers
  - Transactions from critical external parties
- Tier 2 – RTO ≤ 24 Hrs. RPO ≤ 60 Min
  - Critical time sensitive business functions.
- Tier 3 – RTO ≤ 48 Hrs. RPO ≤ 24 Hrs.
  - Enterprise operational efficiency and time constrained functions.
- Tier 4 - RTO≤72 Hrs. RPO ≤ 24 Hrs.
  - Remaining departmental non-time sensitive or non-critical applications.

6.3 IT DR Incident Management Team List

Refer to the table below for the IT DR Incident Management List:

Disaster Recovery Role	Name / Contact Information
IT DR Incident Team Co-Leader	Lydia Ophaug Lydia.ophaug@wellcare.com WP: 813-206-5957
Incident Manager – Infrastructure Storage	Carlos Velasco Carlos.velasco@wellcare.com WP: 813-206-7473
Program Manager - IT-EPC Secondary IT Representative	Matt Hubbard Matthew.Hubbard@wellcare.com WP: 813-206-6040
Incident Manager - Network	Israel Rodriguez Israel.Rodriguez@wellcare.com WP: 813-206-5483
Incident Manager – Infrastructure System Engineers/Unix	Larry Church Larry.church@wellcare.com WP: 813-206-1768
Incident Manager – Infrastructure System Engineers/Windows	Jim Harrison jim.harrison@wellcare.com WP: 813-206-5730
DR Project Manager / EPC IT Primary Representative	Wayne Harrison wayne.harrison@wellcare.com WP 813-206-6771
Lead System Engineer-Storage	Chris Neuner Chris.neuner@wellcare.com 813-206-2119

6.4 IT DR Team

Refer to the table below for a listing of skillsets needed for the IT DR Team Members. The Incident Management team will be responsible to staff team from the availability of resources with the skillsets.

Role	Responsibilities
Network Engineer	1. Manage DR Network 2. Establish DR VPN Profiles for DR Team 3. Execute DR Network Initiation Proc
Unix Engineer	1. Unix Critical System Recovery 2. Back-up Environment Recovery 3. Back-up Restores
AIX/Linux Engineer	1. AIX/Linux Critical System Recovery 2. Back-up Environment Recovery

Role	Responsibilities
	3. Back-up Restores
Windows Engineer	1. Restore MS Exchange 2. Back-up Environment Recovery 3. Back-up Restores
Oracle DBA	1. DR Database Management 2. Replication Services
SQL DBA	1. DR Database Management 2. Replication Services
Enterprise Storage	1. Configure / Allocate DR Storage

6.5 Mission Critical Systems

Refer to the table below for a listing of mission critical systems.

System
Network Infrastructure Disaster recovery network connectivity, WAN / LAN
SRDF Storage-based replication technology that replicates virtual machines to the remote recovery site.
Symantec NetBackUp Master, Catalog, and Media Servers
Site Recovery Manager (SRM) Automated recovery process for Virtual Systems
NAS Shares Network Attached Storage-connected directly to a SAN
WellCare Active Directory Window – root domain controller – houses Active Directory accounts and network configurations.
DR VPN Network opened for application access required by all WellCare Associates
Corporate Email (MS Exchange) Shared company services. Allowing continuation of critical corporate communications.
SharePoint 2010 (WellCare Link) Departmental intranet content including operational procedures and ‘step action plans’.

System
Xcelys / Health Information Portal / Check Run Customer Service, Claims Enrollment, Front End, Benefit configuration, Provider Configuration
CIS (Claims Intake System) Process professional/Institutional CH (FFS) claims
End to End Claims Processing 837 X12 Inbound CH (FFS) claim files through Transaction Manager (X-Engine), Claims Intake System (CIS), Health Information Portal (HIP), Xcelys & Check Run.
CareConnects Address change, Benefits flow, Disenrollment / Reinstatement
Electronic Data Exchange (EDI) Gateway / X-Engine X12 enrollment files, proprietary enrollment files, CMS Enrollment Files; Member Identification files Claims intake process from external vendor
Oracle Financials General Ledger, Payables, Procurement, Purchasing, and Accounts Receivables
Corporate Web (WellCare.com) Member and Provider Portals; Corporate Communication,
WC Toolbox – Appeals & Grievances Appeals and grievances case files, Research denied Authorization/Claim, Member Written Resolution, Vendor Determination Letter
EMMA (Medical Authorizations) Used as an intake and workflow to manage medical authorizations
CPR+ Pharmaceutical System CPR+ is used by Pharmacy to process pharmaceutical authorizations
RightFax Pharmaceutical inbound and outbound case faxes
E2F Medicaid and Medicare member enrollment, claims and billing operations
Sailpoint Identity Access Management (IAM) Provisioning Application
Single Sign-On (SSO) Access control of multiple related systems

System
ESB Controls all web services and supports the Corporate Web, Emma, and Care Connects
Alfresco Works with ESB and controls all web services and supports the Corporate Web, Emma, and Care Connects.
AppXtender Supports Appeals and Clinical Reviews
AutoSys AutoSys is WellCare's "corporate scheduler" used to run jobs and provides event-driven workload monitoring and reporting
Documentum Enterprise Content Management platform for managing the entire information lifecycle
Fulfillment & Correspondence Systems (FCS) A group of applications that produce outbound correspondence with WellCare partners, members and providers) These applications include CTS, VDP, CDS, EOB,RES
Informatica Accesses, discovers and integrates data from the business systems and moves the data throughout the enterprise.
Interqual Evidence based clinical decision support tool
MoveIt Transfers files from one destination to another and tracks file movement through a web interface. Used throughout the Enterprise.
Pega-ClaimsPath Workflow Automation System used throughout the Enterprise.
Pega-CarePath Workflow Automation System used throughout the Enterprise.
Pega-MMP Workflow Automation System used throughout the Enterprise.
SAS Data analytics and business reporting.

System
TFS Team Foundation Servers is WellCare application source code repository
MQ Message transport system allowing program to program communication.
CES (Claims Editing System) Used for outbound claims processing through Xcelys
Encounters Evidenced medical services was provided to members
Citrix Citrix is hot 24/7-365 at or DR data center in New Jersey. At any point in time applications hosted on production network subnets can be launched via Citrix DR. .

6.6 Damage Assessment Form

Area:	Building Structure	Assessment							
		Water Damage		Smoke Damage		Fire Damage		Estimated Repair Time	
No.	Description	Yes	No	Yes	No	Yes	No	Date	Time
1	Roof							/	
2	Ceiling							/	
3	Walls							/	
4	Foundation							/	
5	Raised Floor							/	
6	Sub-Floor							/	
7	Access							/	
8								/	
9								/	
No.	Additional Information								

1	
2	
3	
4	
5	
6	
7	
8	
9	

Area:	Environmental Systems	Assessment			
		Physical Damage		Estimated Repair	
No.	Description	Yes	No	Date	Time
1	Heating			/	
2	Cooling			/	
3	Water			/	
4	Power			/	
5	Fire Suppression			/	
6				/	
7				/	
8				/	
9				/	
No.	Additional Information				
1					

2	
3	
4	
5	
6	
7	
8	
9	

Area: IT Systems		Assessment			
		Physical Damage		Estimated Repair	
No.	Description	Yes	No	Date	Time
1	Servers			/	
2	Storage			/	
3	Voice			/	
4	Network Components			/	
5				/	
6				/	
7				/	
8				/	
9				/	
No.	Additional Information				
1					
2					
3					
4					

5	