Disaster Recovery

&

Business Continuance Plan

Prepared By:

DBMS I/T

Revised: 5/1/2013

THIS DOCUMENT CONTAINS PROPRIETARY AND CONFIDENTIAL INFORMATION OF DBMS, INC. AND ITS AFFILIATES. THE INFORMATION CONTAINED IN THIS DOCUMENT MAY NOT BE DISCLOSED OUTSIDE YOUR COMPANY WITHOUT THE PRIOR WRITTEN PERMISSION OF DBMS, INC.

These are the main components to the Disaster Recovery document.

- Disaster Recovery & Business Continuance Processes
- Disaster Recovery Exercise (Schedule A)
- Business-Continuity and Disaster-Recovery Services (Schedule B)

1. *Planned outages*

On occasion, IT needs to interrupt one or many services for maintenance purposes. As part of the Business Continuance process, communicating the scheduled interruption and acquiring permission is key in avoiding Business interruption.

All system updates are scheduled with the Client's I/T in advance. When installing system updates, and after completing a unit/full test by DBMS' I/T and, if necessary Client's Testers, the client's I/T project manager will receive a message to inform the Client's users of the new changes. They may then sign off then back into the system, if they would like to use some of the new system updates/enhancements immediately, especially if such changes are applicable to their business area. This concept minimizes the downtime and interruption during normal business hours. Major release updates take place after business hours or over the weekend and will include Client participation in Testing.

2. *Electrical Power*

Our internal ability to ensure the stability and manageability of electrical power is an integral part of hardware and information protection. Electrical power supplied to servers is routed through an Uninterruptible Power Supply unit (UPS). An UPS will protect the servers from fluctuations in power that could damage hardware or cause the server to shutdown unrepentantly (Dirty Shutdown). In the rare event servers need to be shut down, graceful shutdowns initiated by in interruption in electrical power will be in place for all servers.

3. *Hardware Failures*

Hardware failures are unpredictable but can be avoided. The continual refreshment of hardware with reputable products can significantly reduce hardware failure but will not eliminate them. Our ability to respond to hardware failures is critical in Business Continuance.

Reasonable hardware failure response time can be reached by establishing relationships and contracts with suppliers to provide replacement parts and units within pre-established time frame. Either these contracts will be in place and /or spare parts / units will be kept on site. The contracts and parts will be reviewed and be verified at least once a year.

There will be replacement plans, such as having an extra server and a secondary data center site (hot-site) location, will be in place with the replacement equipment being large enough to handle the demands of any existing mission critical applications..

4. *Data Backup and Restore*

Data Backup and restore is a basic operation of any business using computers. Data backups are performed diligently. This will be combined with monitoring and testing.

Restore testing will be broken down into two categories. The first is a local test of restore success as discussed earlier. The second is a foreign test of restore success.

The foreign restore test is required to ensure that the data stored on media can be restored using similar equipment in a facility not in the region where the data is currently in use. This type of testing will verify that tape drives are not misaligned whereby the data stored on the tape can successfully recovered with the drive used to write the data. In case of a disaster, the drive used to write the data will most likely not be available for restore functionality. Cross regional exchange of media can accommodate this type of testing. Client must also commit to this testing.

5. *Off-Site Virtual/Media Storage & Backup Sites*

Storing backup media Off-Site is essential in our ability to recover from a disaster whereby the facilities where the computing resources are located are no longer accessible (fire, flood, structural damage, etc.). In addition, DBMS has duplicated its core servers to run at a secondary site location, over 50 miles away from the main Indianapolis location, in order to point to a separate server (data center) in case of a major failure. DBMS' I/T and clinical staff are set-up to work remotely from home or another remote location, in the event of a natural disaster.

6. *Security*

Applicable security services (encrypted data security and username/password). Off site / hot site locations will have, at a minimum, the same level of security as the primary site.

7. *Off-Site Facilities*

We have off-site service configured in Pittsburg, PA and another undisclosed hot-site location. These facilities utilize snapshot technology and have a snapshot of our servers (all drives) that allow us to restore current data (that gets imported into various virtualization environments), backed up properly in order for such backup servers to run within 48 hours in the event of a major disaster, as indicated below.

- Indianapolis, IN (Main development, support, and data location)
- Pittsburgh, PA (Production will be recoverable at SUNGUARD)
- Undisclosed hot-site services (Snapshot image ready for recovery).

Schedule A
Disaster Recovery

1. Introduction

The core subject of this document focuses on the DBMS Server(s) that support and maintain DBMS' Integrated Care Management System (ICMS/eCARE applications), its continuous accessibility and maintenance/support procedures in case of a disaster.

1.1 Precedence of Obligations. The Parties acknowledge that certain obligations may be set forth in both this Schedule and elsewhere in this or the DBMS Software License Agreement.

1.2 Section References. Unless otherwise specified, Section references in this Schedule refer to the Sections of this Schedule.

1.3 Definitions. Capitalized terms used and not otherwise defined in this Schedule have the meanings given them in the Agreement.

2. DBMS Disaster Recovery Objectives

This document contains the scope, scenario, objectives, assumptions, and success criteria for the DBMS's disaster recovery exercise (the "**Disaster Recovery Exercise**"). It was leveraged from the scope, scenarios, objectives, assumptions and success criteria for DBMS's 2009 disaster recovery exercise.

Items related to Supplier's participation and responsibilities in the Disaster Recovery Exercise are labeled as "DBMS". These were primarily WISHARD's roles and responsibilities in DBMS's disaster recovery exercise related to the Servers and Server recoveries and support of the recovered environments for which DBMS will have responsibility in the production environment, such as online processing, interfaces/integration, monitoring/support, etc.

DBMS will be responsible for distributed server and application recoveries for which they will retain responsibility in the production environment, such as ICMS-Server, ICMS database, etc.

Dedicated network connectivity (Citrix and VPN) between the DBMS network and SunGard (or others) will need to be in place prior to the Disaster Recovery Exercise. The completion of this will be a shared responsibility between SunGard, DBMS, and WISHARD. Both networks must be place and will be tested in the Disaster Recovery Exercise.

One 48-hour exercises will be scheduled by DBMS (in advance) For scheduling purposes, dates that the DBMS business units can support and/or execute these exercises will be between October 15 – 30th of 2011.

EXERCISE SCOPE

The purpose of this document is to outline the associated exercise activities to test the recovery capabilities of both DBMS and Wishard.

This exercise will recover the following computing environments which have been made available at the DBMS Indianapolis data center, and at the SUNGARD site:

- Production servers (ICMS SqlServer)
- Selected Active Directory and Domain servers (DBMS Exchange Server)
- DBMS CRONOS (Development and Test server)

This recovery exercise will also include the following changes related to secondary objectives to be pursued if time permits:

- None at this time. These can be requested by WISHARD and will be accommodated as time and resources permit.

DBMS DISASTER RECOVERY EXERCISE

– 2010 SCOPE – OBJECTIVES – SUCCESS CRITERIA

EXERCISE SCENARIO

The Disaster Recovery Exercise will be performed based on the following disaster scenario.

- The Castle Creek Data Center building was destroyed by fire; no other buildings on the Castle Creek campus are affected.
- All required DBMS and DBMS staff members are available to perform recovery tasks.
- DBMS is responsible for media in offsite storage facilities and data rotation was performed prior to the disaster.
- All documentation located in the Castle Creek Data Center was destroyed, offsite documentation will be used.
- DBMS is responsible for providing equipment, directly or as contracted with SunGard, at the SunGard Recovery Center as required for a successful test.
- Other DBMS computing data centers are functioning as normal.

EXERCISE OBJECTIVES

If both DBMS and WISHARD primary objectives are successfully accomplished and the actual results of the Disaster Recovery Exercise achieve the Success Criteria, then both DBMS and WISHARD will consider the Disaster Recovery Exercise a success.

DBMS OBJECTIVES - PRIMARY

- Test predetermined distributed application connectivity through the gateways to the server environment.
- Test predetermined distributed applications on selected distributed equipment.
- Establish data network connectivity between the SUNGARD recovery facility and the following:
    - DBMS Indianapolis, IN (main development & support location)
    - DBMS Pittsburgh, PA (production services)
    - WISHARD

- Configure network router to manage out-bound data traffic from the exercise facility.

- Provide DBMS the Citrix and other configuration for equipment in Indianapolis, IN:
    - prevent exercise traffic from accessing production environment
    - provide for server print capability in Indianapolis, IN.

- Provide network connectivity between SUNGARD and Indianapolis, IN Provide network connectivity for distributed equipment located on DBMS campuses:
    - Acceptance servers in Indianapolis
    - Development server in Indianapolis
    - DBMS Domain server in Indianapolis
- Coordinate the use of the following servers for the exercise:
    - Acceptance servers in Indianapolis
    - Development server in Indianapolis
    - DBMS Domain server in Indianapolis
    - Server Equipment at SUNGARD
- Provide DBMS the Disaster Recovery Exercise workstation configuration for workstations in Castle Creek.
- Manage, distribute and/or destroy any printed reports originating from the Disaster Recovery Exercise and printed in Indianapolis, IN.
- Perform recovery of report distribution databases
- DBMS will identify server applications and associated run schedules that will be tested
- For applications being recovered, the exercise will consist of the following activities:
    - verify applications are operational and functional against known criteria.
    - verify all required data is available / accessible for exercising.
    - execute jobs as required to simulate production requirements

DBMS OBJECTIVES - SECONDARY

- None

DBMS PRIMARY OBJECTIVES

- DBMS will restore the server computing environment and turnover the environment to DBMS 24 hours prior to the end of the Disaster Recovery Exercise-for the validation of the identified critical production applications.
- DBMS will coordinate delivery of backup tapes (or will verify virtual backup data and configuration) remotely or in person.
- DBMS will restore data from the targeted backup tapes (or virtual backup).
- DBMS will follow the problem reporting procedures as outlined in the Disaster Recovery Plan**.**
- DBMS will follow the status call procedures as outlined in the Disaster Recovery plan.
- DBMS will provide operational support for the recovered systems as in the production environment

DBMS SECONDARY GOALS

- None

OUT-OF-SCOPE OBJECTIVES

- Recovery of computer processing environments in other DBMS locations
- Recovery of voice communications
- Recovery of business work areas
- Recovery of test/acceptance/development data and systems
- Recovery of Warehouse data
- Connections to 3rd party vendors
- Print from Castle Creek print center using Info-print (if applicable)

DISASTER RECOVERY EXERCISE ASSUMPTIONS

The following issues and assumptions are critical to the timely completion and success of the Disaster Recovery Exercise.

SUNGARD has installed allocated and verified server and distributed equipment for the exercise.

- DBMS will identify the applications that will be tested during this exercise.
- DBMS will not be held accountable for missing any associated Service Levels as a result of DBMS staff accessing the Disaster Recovery environment prior to formal turnover nor shall DBMS be held accountable for any associated Service Level Credits.
- DBMS will make available the off-site tapes required for the application recovery process.
- Connection is available to Indianapolis, IN, via Citrix and other equipment.
- All service level agreements and their measurements are not applicable to this exercise.
- DBMS will identify the critical applications that will be recovered during this exercise.
- DBMS is responsible for the documentation and procedures to be used in the testing of the application recovery process.
- DBMS is responsible for notifying external sources (for which they hold employment, contract, and/or agreements with) of this Disaster Recovery Exercise.
- Time permitting; secondary objectives will be attempted as part of the exercise; however the results of the secondary objectives will not affect the success/failure of the exercise.
- Disaster Recovery Test environment for the DBMS' ICMS application will not support entire user community.
- DBMS will be responsible for performing the backup and recovery of the SQL databases.
- DBMS will provide for an outage window on the selected distributed servers to perform Disaster Recovery backups. Outage window must be at the same time for all servers that require backups.

SUCCESS CRITERIA

The actual results of the Disaster Recovery Exercise will be categorized as follows:

Unsuccessful
Partially Successful
Successful!
Exceeded Expectations!

The Disaster Recovery Exercise will be deemed to have achieved the Success Criteria if and only if the results for each of the Success Criteria are either "Successful!" or "Exceeds Expectations." The Disaster Recovery Exercise will not be deemed to have achieved the Success Criteria if the results for any of the Success Criteria are either "Unsuccessful" or "Partially Successful."
A description of the Success Criteria by component follows. Success Criteria for DBMS tasks and responsibilities has been highlighted in **BOLD BLACK** and is noted as *****DBMS is responsible.**

WISHARD Testers will, upon completion of any Disaster Recovery Exercise within the overall test, promptly report to DBMS as to the results of the Disaster Recovery Exercise with respect to each of the Success Criteria.

NETWORK

Isolation (rated for duration of the exercise)	**Unsuccessful**	Access allowed outside Disaster Recovery environment (DBMS production, outside DBMS network)
	Partially Successful	
	Successful!	No access allowed outside Disaster Recovery Environment
	Exceeded Expectations!	No network support actions needed to maintain isolation during the exercise

System Connectivity (rated for duration of the exercise)	**Unsuccessful**	No connectivity between any recovered systems
	Partially Successful	Connectivity to up to 85% of recovered systems (including pinging)
	Successful!	Connectivity to 86 – 100% of recovered systems (including pinging)
	Exceeded Expectations!	Data exchanges between recovered systems

User Connectivity (rated by site for duration of testing)	**Unsuccessful**	No workstation connectivity between any recovered systems
	Partially Successful	Workstation connectivity to up to 85% of recovered systems (including pinging)
	Successful!	Workstation connectivity to 86 – 100% of recovered systems (including pinging)
	Exceeded Expectations!	No network support actions needed for user connectivity during the exercise

SERVER's & Mainframe's

Met the Build SLA **(rated by LPAR)** *****DBMS responsible**	**Unsuccessful**	**LPAR (per customer's requirement) not built w/in SLA (48 hrs)**
	Partially Successful	**Up to 85% of LPAR built w/in SLA (48 hrs)**
	Successful!	**LPAR built by SLA (48 hrs)**
	Exceeded Expectations!	**LPAR built in less than SLA (<48 hrs)**

DISTRIBUTED SERVER BUILDS

DBMS (rated by Server)	**Unsuccessful**	Server not built w/in SLA (48 hrs)
	Partially Successful	Up to 85% of Server built w/in SLA (48 hrs)
	Successful!	Server built by SLA (48 hrs)
	Exceeded Expectations!	Server built in less than SLA (<48 hrs)

APPLICATIONS

(ICMS & other eCARE - rated by application)

IT Verification	**Unsuccessful**	Application not recovered
	Partially Successful	Up to 85% data restoration & functionality
	Successful!	86 – 100% data restoration & functionality
	Exceeded Expectations!	
User Verification	**Unsuccessful**	Application unavailable for testing
	Partially Successful	Up to 85% data restoration & functionality
	Successful!	86 – 100% data restoration & functionality
	Exceeded Expectations!	

HL7, other Real-Time, or Batch Processing

*****(shared with DBMS)**	**Unsuccessful**	**Unable to complete real-time or batch processing**
	Partially Successful	**Up to 85% of planned real-time or batch jobs processed**
	Successful!	**86 – 100% of planned real-time or batch jobs processed**
	Exceeded Expectations!	
Interface with other	**Unsuccessful**	Unable to interface with appropriate
	Partially Successful	
	Successful!	

Applications (HL7 - in scope as planned)		applications
		Up to 85% of interfaces successful
		86 – 100% of interfaces successful

ADDITIONAL SUCCESS CRITERIA for DBMS' ICMS

Database Recovery (rated by Database)	**Unsuccessful**	Not recovered
	Partially Successful	Up to 85% data restoration & functionality
	Successful!	86 – 100% data restoration & functionality
	Exceeded Expectations!	

Staffware Recovery	**Unsuccessful**	Not recovered
	Partially Successful	Up to 85% restoration & functionality
	Successful!	86 – 100% restoration & functionality
	Exceeded Expectations!	

FAXing (RightFax, if applicable)

Unsuccessful	No FAXes sent/received
Partially Successful	Up to 85% of FAXes sent/received
Successful!	86 – 100% of FAXes sent/received
Exceeded Expectations!	

Schedule (B)

Business-Continuity and Disaster-Recovery

	BUSINESS-CONTINUITY AND DISASTER-RECOVERY SERVICES	Customer Obligations
	Business Continuity	
	Customer will retain responsibility for its Business-Continuity plans and management activities. Supplier will describe its business continuity plans as needed by Customer. Supplier will assist Customer in Business-Continuity planning and testing as it relates to the Services. To the extent that the Disaster-Recovery Services included as part of Supplier's scope are included as part of Customer's overall Business-Continuity plan, Supplier will also be supporting that plan. Supplier will also share its business-continuity methodology with Customer to assist Customer in validating its overall business-continuity process.	Develop and Maintain Business-Continuity Plans.
	The Supplier's responsibilities include:	
	1.0 Updating, maintaining, managing, testing and implementing any portion of the Business-Continuity plans and activities that relate to the continued provisioning of the Services.	
	2.0 Disaster-Recovery Planning	
	Customer will provide the requirements (i.e., Recovery Time Objective/Recovery Point Objective) by which Supplier will develop the Disaster-Recovery Plans for the Services Supplier provides with Customer having final review, approval and oversight of the Supplier Disaster Recovery Plans, Supplier Disaster Recovery exercise. and corrective action plans Customer will Approve all Disaster Recovery plans and modifications to such plans.	Provide and distribute requirements and Disaster Recovery objectives and approve Disaster-Recovery Plans.
	The Supplier's responsibilities include:	
	1. Updating, maintaining, managing, testing and implementing any portion of the Business Continuity plans and activities that relate to the continued provisioning of the Services. 2. Effectively managing and maintaining the Disaster-Recovery Plans of Customer, as they exist on the Effective Date. Supplier will maintain the current recovery procedures, including through if applicable, the use of any Customer recovery vendor agreement(s), during the applicable Transition Period. Supplier will use Customer's current recovery vendor agreement(s), if applicable, to provide Disaster Recovery Services for the Servers until such agreement(s) expire(s). Supplier will then renew or replace that agreement(s) with an equivalent capability.	
	3. Performing a gap analysis of Customer's Disaster-Recovery Plans that exist on the Effective Date, and developing rationale and recommendations to address any perceived gaps.	
	4. To the extent that Customer does not have a documented Disaster-Recovery Plan encompassing all Services, Supplier will develop and implement a Disaster-Recovery Plan using the Supplier's best practices	

		and standards for companies of similar industry, size, and services. Supplier will provide a customized disaster recovery approach for Customer's Mainframe and Server environments, which takes advantage of the increased resiliency available through Supplier's dual data-center solution.	
	5.	Customer will approve any such Disaster-Recovery Plan developed by Supplier and will provide support in creating the plan	Review and approve Disaster-Recovery Plan.
	6.	Maintaining and continually enhancing the Supplier's Disaster-Recovery Plans throughout the term of the Agreement, including:	
	7.	Enhancements required due to the introduction and use of new technologies (Equipment, Systems Software, Applications Software, etc.), Resource Units, processes, business functions, locations, and priorities. *7.1 Maintain Disaster Recovery contracts (during the migration from one location or system to a new environment the Disaster Recovery contracts will be modified to reflect the changes.)* *7.2 Conduct annual Disaster-Recovery Plan review with Customer.* *7.3 Execute Disaster-Recovery exercises.* *7.4 Subject to the availability (Customer and Disaster Recovery site) coordinate the scheduling of annual Disaster-Recovery exercise.* *7.5 Develop a customized Disaster-Recovery Test Plan for each Disaster-Recovery exercise.*	

	7.6 Mutually define the scope and success criteria for each Disaster-Recovery exercise. *7.7 Establish joint test objectives to verify that Customer Systems will be available within an established timeframe.* *7.8 Provide technical resources to recover the existing Disaster-Recovery solution.* *7.9 Work jointly with Customer to develop a customized Disaster-Recovery post test review plan for each Disaster-Recovery exercise.* *7.10 Provide Customer with a formal report of the test results within thirty (30) days of each test.* *7.11 Execute disaster declaration.* *7.12 Report Disasters (or potential Disasters) to Customer immediately upon identification based on parameters defined in the Disaster-Recovery Plan, and consult with Customer for an official declaration of a Disaster as appropriate.* *7.13 Focal point for all teams (Disaster Recovery site, Supplier crisis management team, Supplier recovery team, Customer contingency planning*	

	coordinator). *7.14 Assign Supplier technical resources to recover the existing Disaster-Recovery solution.* *7.15 In accordance with the Disaster-Recovery Plan, and in conjunction with Customer determine what resources to deploy; and conducting, supervising, and administering the operation and implementation of such resources.* *7.16 Provide focal point for the move back to primary data center after facilities or mutually agreed upon alternate site is ready.* *7.17 Following any Disaster, conducting a post-Disaster meeting with Customer in order to understand that cause of the Disaster; and developing plans to eliminate or mitigate future occurrences.* *7.18 Recovery times will be as required by Customer in accordance with the approved Disaster-Recovery Plan.* *7.19 Supplier understands that the in-scope organization has enterprise-wide Disaster Recovery planning and testing and confirms that it will assume these functions.*	

	7.20	*Integrating the Disaster-Recovery Plans related to the Services with any company-wide Business-Continuity plans and activities of Customer.*	
	7.21	*Documenting the manner and procedures by which the Supplier will perform backups without impacting production availability, provide Disaster-Recovery Services and assist with Business Continuity.*	
	7.22	*Documenting Customer's priorities for recovery, Disaster-Recovery and Business Continuity based on the priorities established by Customer.*	
	7.23	*Documenting the methods and timeframes that allow Customer to change priorities.*	
	8.	With Customer's input and approval, developing a process that will determine and modify the list of mission critical Applications on an annual basis.	.
	9.	Working with Customer to incorporate security measures, as defined for normal operations.	
	10.	Maintaining a list of key personnel contacts and notification procedures for Customer, the Supplier, and Third Party Vendor personnel.	
	11.	Providing a single point of contact for Business-Continuity and Disaster-Recovery Plans, related communications and other activities that are the Supplier's responsibility.	
	2.1	**Disaster-Recovery Testing**	
	The Supplier's responsibilities include:		
	1.	Working with Customer to establish joint test objectives to verify that Customer's Systems will be available within an established timeframes.	.
	2.	Subject to the availability of a Customer-designated test site(s), scheduling and testing all components of the Disaster-Recovery Plans at least annually in cooperation with Customer, its designees, any testing and recovery providers, and any other Third Party Vendors providing services to Customer.	
	3.	Scheduling testing dates with Customer's approval and giving Customer and its representatives the opportunity to observe and participate in the tests.	
	4.	Coordinating and administering Third Party Vendors utilized by Customer during testing in accordance with the Disaster-Recovery	

		Plan(s).	
	5.	Continuing to operate and manage the Services during periodic Disaster-Recovery tests.	
	6.	Providing Customer with a formal report of the test results within thirty (30) days of each test. At a minimum, these reports should include:	
		6.1 The results achieved.	
		6.2 A comparison of the results to the measures and goals identified in the respective Disaster Recovery requirements and objectives outlined in the Approved plan.	
		6.3 A report on the feedback from Authorized Users as to the adequacy of continuity for their respective areas.	
		6.4 A plan and a schedule to remedy any gaps or identified failures revealed during testing submitted to Customer within 45 days.	Need to Check SLAs
	7.	Retesting the failed component within (i) ninety (90) days, or (ii) the earliest possible date available at the applicable DR vendor site, if any disaster simulation(s) fails to achieve specified results due to the Supplier's failure to perform its responsibilities. Reporting to Customer upon retesting and verifying that the remedy was successful.	
	2.2	**Disaster-Recovery Activities**	
	The Supplier's responsibilities include:		
	1.	Reporting Disasters (or potential Disasters) to Customer immediately upon identification based on parameters defined in the Disaster-Recovery Plans, and consulting with Customer for an official declaration of a Disaster as appropriate.	
	2.	For all facilities where the Supplier has oversight responsibility, declaring Disasters in accordance with procedures existing at the time of declaration and notifying Customer of situations that may escalate to Disasters as soon as practicable.	
	3.	Executing the Disaster-Recovery Plans including assumption of the responsibility to operate the Equipment; restoring the Software; verifying that data is recovered to the appropriate point in time; and providing all other functions associated with the Services.	
	4.	In accordance with the Disaster-Recovery Plans, determining what resources to deploy; and conducting, supervising, and administering the operation and implementation of such resources.	
	5.	Providing additional resources as necessary to maintain provision of the Services for unaffected areas and realigning technical resources to maintain Business Continuity.	
	6.	In accordance with the Disaster-Recovery Plans, coordinating and	

		administering Third Party Vendors utilized by Customer.	
	7.	Following any Disaster, conducting a post-Disaster meeting with Customer in order to understand that cause of the Disaster; and working with Customer to develop plans to eliminate or mitigate future occurrences.	
	8.	Whether a Disaster-Recovery Plan exists or not, at a minimum restoring the Services within a timeframe that is expected in the industry from large, well-managed outsourcing services companies.	
	2.3	**Other Disaster-Recovery Activities**	
	The Supplier's responsibilities include:		
	1.	Negotiating and managing contracts with Third Party Vendors providing Disaster-Recovery services, as agent for Customer to the extent permitted by the third-party agreements.	
	2.	At all times, maintaining strict compliance with the Disaster-Recovery policies, standards and procedures contained in Customer's Disaster-Recovery Plans. Supplier will have operational and financial responsibility for Disaster-Recovery in accordance with the Services stated in Section 12.0 (Business-Continuity and Disaster-Recovery Services) of thus Exhibit 2.1. (Cross Functional-General Services).	
	3.	Training Supplier and Customer personnel in Disaster Recovery procedures and implementing a process to obtain immediate access to such procedures in a disaster situation.	
	4.	For Server and Mainframe Services, providing and maintaining backups; file recovery capabilities; and historical files of data and Software (including source code; provided, in the case of Software not provided by Supplier, Customer has provided Supplier with source code) utilized to process data for the purpose of offsite recovery. Additional responsibilities will include:	
		4.1 Adhering to the time periods specified for recovery by Customer in the Disaster-Recovery Plan.	Define time periods for recovery.
		4.2 Using magnetic media, or other media approved by Customer and accessible to Customer.	
		4.3 Performing the required functions to interface with the off-site storage third party services supplier or providing off-site storage in a secure facility for the foregoing, as well as daily pickup and delivery to the off-site storage site.	
		4.4 Performing such functions in accordance with standards and procedures in the Disaster-	

	Recovery Plans, and being no less stringent than the standards and procedures used at well-managed companies providing similar backup and recovery features for similar services.	
	5. Supporting connectivity to Customer's mission-critical production network and the production host Systems or to the contingency network and the recovery sites as required by the Disaster-Recovery Plans, provided that Customer will retain responsibility for connectivity to the SunGard Disaster Recovery site prior to the expiration of Customer's Disaster Recovery agreement with SunGard.	
	6. Providing design and other consulting support for networking requirements at the contingency site, including such support for local connectivity to required Servers and printers.	
	7. Supporting connectivity from Supplier's contingency site to all external Suppliers and other organizations, as required by the Disaster-Recovery Plans.	