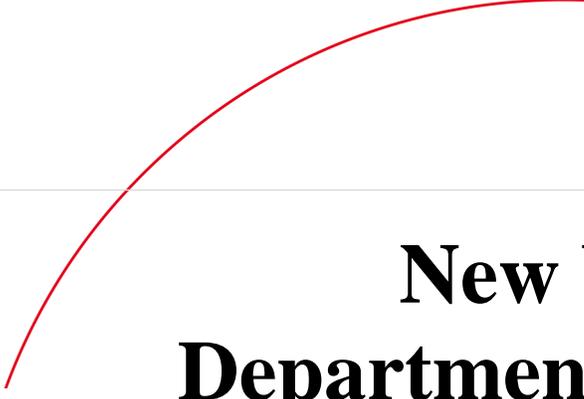


New York Health Benefit Exchange

Detailed Design Review Summary for 9.7.7 Contingency / Recovery Plan October 9 & 10, 2012

Item Number	Topic
9.7.7	Contingency / Recovery Plan

A decorative red curved line that starts near the top left and arcs towards the right, partially overlapping the text.

New York State Department of Health

NY-HX Project

Computer Sciences Corporation

Error and Disaster Recovery Draft Plan

Release PRELIMINARY
Date Submitted: July 3, 2012

Table of Contents

1	The NY-HX Error and Disaster Recovery Plan.....	1
1.1	Scope of Plan	1
1.2	CSC Commitment to Preventing/Mitigating Problems.....	1
1.3	Severity of Disaster.....	1
1.4	State Interfaces.....	2
1.5	Security	2
2	CSC’s First Response to Emergency Situation.....	3
2.1	Assessment of Severity of Disaster.....	3
2.2	Establishing the Control Center	3
3	Systems Administration	4
3.1	Disaster Preparedness	5
3.1.1	Mainframe / Midrange	5
3.1.2	Backups.....	5
3.1.3	Checkpoint/Restart Capabilities.....	6
3.1.4	Offsite Storage and Retention	7
3.1.5	Help Desk.....	7
3.1.6	Documentation	7
3.1.7	Telecommunications	7
3.2	Disaster Recovery Procedures	7
3.2.1	Assessment.....	7
3.2.2	Facilities and Staffing	8
3.3	Restoration Procedures	9
3.3.1	Repair Primary Site.....	10
3.3.2	Restore Hardware.....	10
3.3.3	Restore Software.....	10
3.3.4	Move Data.....	10
3.3.5	Notification	10
3.3.6	Switch Telecommunications	10
3.3.7	Relocate Staff.....	10
3.3.8	Resume Production in Primary Facility	10
3.4	Disaster Preparedness Testing	11
3.4.1	Scope of Testing.....	11
3.4.2	Location of Test	11
3.4.3	Testing Procedures.....	11
3.4.4	NYS Review of Test Results	11
	Appendix A – Management Team (MT)	12
	Appendix B – Contingency Assessment Team.....	15
	Appendix C – CSC Disaster Recovery Operations Team (DR).....	17
	Appendix D – Assessment Charts	19
	Appendix E – Preliminary Vendor List	24
	Appendix F – Disaster Recovery Site Configuration List	26
	Appendix G – Implementation Plan.....	27
	Appendix H – Disaster Recovery Site Connectivity	38
	Appendix I – NY-HX Data Center Configurations	39



1 The NY-HX Error and Disaster Recovery Plan

This document represents how the NY-HX team will prepare for the eventuality of a disaster, the procedures to be followed during a disaster, how operations would be restored to the primary facility, and testing procedures.

1.1 Scope of Plan

This plan covers natural or man-made disaster situations that fall short of the “*Force Majeure*” provisions defined in the NY-HX Funding Availability Solicitation. CSC assumes that the State has backup plans to cover the widespread disruptions of service that would result from such catastrophic events.

CSC addresses a limited disaster by assessing the specific situation and activating our preparedness plans in the order and to the degree required, providing essential services to NY State citizens. CSC’s plan allows for flexibility in our recovery modes to account for differing situations. In any event, CSC’s approach is to restore absolutely essential services first, as prioritized in close consultation with Health Department Leadership.

1.2 CSC Commitment to Preventing/Mitigating Problems

CSC’s design for the NY-HX system prioritizes *preventing* a major loss of service, or to minimize the effects of a failure, rather than to react to a difficult situation once it has occurred. For this reason, NY-HX incorporates a redundant infrastructure, along with disciplined quality assurance efforts. CSC’s Quality Assurance Plan outlines these details.

The hardware and software components of the system are based on advanced and proven technologies. The data center has been designed with redundancy built into every major subsystem. The application software is parameter and table-driven so as to minimize the possibility of programming errors being introduced when changes and enhancements are made to the system. It is well known by experienced system developers that the most likely cause of errors introduced in the development or enhancement of systems is hard coded program logic. The use of table and parameter driven logic greatly reduces the risk of errors by eliminating the use of individual program instructions to perform specified functions. We have provided for off-site software and data storage, as well as off-site processing capability in the event that it becomes necessary.

1.3 Severity of Disaster

As total disasters are considered unlikely, CSC’s approach emphasizes assessing the extent of a problem, and addressing it in the context of that severity.

CSC has organized its response to an emergency or disaster around a team approach. Teams have been designated, duties assigned, and members selected based on the function of each team and the skills required. The makeup of our teams is described in more detail in Section 2 and in Appendixes A through C.

The CSC Assessment Team (AT), in conjunction with vendor support, would handle initial assessment of a disaster situation. After initial assessment of the general situation, individual departmental plans would come into play. Therefore, each of the plans that follow contains its own section addressing incident assessment activities that would be specific to a particular portion of the NY-HX system. Even so, it is very difficult to predict all possible scenarios, and therefore our plans include sufficient flexibility to determine the most effective response to a specific situation.



1.4 State Interfaces

CSC recognizes the importance of the Contractor/State partnership, especially during an incident that would fall under this plan. We have included and planned for the involvement of State personnel at all levels as our response to a situation develops. CSC and the Department will jointly determine when unscheduled system downtime is to be elevated to a disaster status. CSC actions will be taken with the full cognizance of the State. Our primary contacts with State staff have been listed in Appendix A, and will be updated, as required.

1.5 Security

The very nature of an emergency or disaster, regardless of scope, raises serious issues of security. CSC is aware that during the emergency and subsequent recovery operations, there will need to be a heightened awareness of security concerns. During staff training for emergency operations we emphasize the importance of maintaining physical and data security, especially during data transport operations, should they be needed.

Data Security for the NY-HX is focused on the *Confidentiality, Integrity and Availability* of Personally Identifiable Information (PII), Protected Health Information (PHI), and Federal Tax Information (FTI) pursuant to the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (“HITECH”), IRS Section 6103 and various State Regulations.



2 CSC's First Response to Emergency Situation

The activities described in this section are those that would take place early on in any emergency or disaster situation. These are mostly management-level activities that would be a precursor to implementing individual action plans by area.

2.1 Assessment of Severity of Disaster

As soon as it is apparent that a disaster has occurred, CSC will convene the CSC Management Team (MT) and a Contingency Assessment Team (AT) at the primary site. These teams will rapidly determine the extent of the emergency, call upon other staff as necessary to provide detailed information and options, converse with State contract monitoring personnel, and make joint decisions with the State as to the scope of the problem and appropriate initial responses.

The CSC MT will include the Account Executive, Account/Contract Manager, and the manager of each CSC NY-HX and eMedNY departments. The MT's role includes alerting the backup site and off-site storage vendor of a potential disaster, activating the AT and providing overall leadership at the site. The AT will assess the damage to the facility and advise the MT on the course of action to be taken. The MT and State of New York Department of Health representatives will then jointly decide which departments need to activate their disaster recovery plan(s), and deploy to their backup location(s). All subcontractors and vendors that will be affected, and were not needed as part of the assessment team, will be notified. CSC employees will be informed of changes to their operation or work location.

Those areas that have been affected will then call upon their own designated disaster recovery teams to assess the scope of relocation/recovery operations.

The makeup of the CSC Management Team is shown in Appendix A. The makeup of the Contingency Assessment Team is listed in Appendix B.

2.2 Establishing the Control Center

When the Disaster Recovery Management Team has concluded that a disaster within the NY-HX facility has occurred which will necessitate implementation of backup plans for specific functions, the team will establish a Control Center as soon as possible to provide a central facility for monitoring and controlling all disaster recovery activities. Location of the Control Center will depend on how extensive the damage is to the Columbia Turnpike facility. The Control Center will house the Management Team for the duration of the recovery period. The primary choice for location of the Control Center is the present facility at Columbia Turnpike. However, if the current facility is damaged so severely that it would not accommodate such an operation, the secondary choice for the Control Center will be at the Riverview Center at 150 Broadway in Menands, NY and if that is not available, a local hotel or other facility within a 20-mile radius of Albany. CSC has identified several appropriate sites that could accommodate the Management Team.



3 Systems Administration

The objective of this plan is to ensure New York State health insurance exchange business functions continue in the event that the entire facility, or a portion of it, is rendered inoperable as result of a natural, accidental or international disaster.

CSC focused on a high availability operation when designing a data center for the NY-HX. CSC has selected equipment with a high level of reliability and redundancy. The business continuity, backup, failover and disaster recovery features of the NY-HX leverage the eMedNY Private Cloud VMware, guest images and data replication environment, already in place between the Rensselaer Data Center and the SunGard DR facility in Carlstadt, NJ.

This configuration benefits business continuity with minimal downtime due to hardware failure. When hardware problems are detected on an individual component, the failover components are in place to assume the system's workload.

Primary data storage is provided by Hitachi VSP storage systems, with redundant power supplies, non-disruptive macrocode upgrade capabilities and non-disruptive hardware component replacement. This means the microcode on these units can be upgraded without taking the storage offline or interrupting processing.

A copy of critical application and Operating System data will be created at the disaster backup facility. In addition, the offsite copy will have a mirror image made. The use of mirroring and remote copy will provide the highest data availability for NY-HX applications.

The data is created at the disaster backup facility through the use of two Gigabit Ethernet connections, deployed to ensure redundancy, and utilizing different vendors to eliminate single-point-of-failure concerns.

All critical host servers in the hardware configuration have a redundant power supplies and dual network feeds. In addition, components critical to the ability of the Call Center to access the NY-HX system, such as network access servers, routers and firewalls; have redundancy built into the network configuration.

The CSC Data Center includes the provision for equipment that will provide electrical power to support the NY-HX operation in the event of power failures. The Data Center is equipped with dual Uninterrupted Power Supplies (UPS) and a diesel-powered generator to provide state-of-the-art continuous backup power until normal power is restored.

Subcontractor/Vendor Involvement

Emergency phone numbers for Police and Fire Departments are also included. Vendors and Subcontractors to CSC are expected to be under a contract or maintenance agreement with CSC to provide routine services applicable to normal operations, or have been committed to provide services in the event of a disaster. All firms that support functions affected by the disaster will be contacted by the Contingency Assessment Team, informed of the disaster, and notified of any interim operating procedures that will be followed during the recovery period.

3.1 Disaster Preparedness

This section describes the provisions that CSC Systems Administration is making for the possibility of a disaster. These activities are key to a successful reaction to a real disaster, as they provide for the systems, data, and staff support that would be deployed.

3.1.1 Mainframe / Midrange

Some NY-HX components leverage the existing eMedNY mainframe and Midrange systems environments. In the event of a disaster, CSC has arranged with SunGard Availability Services (hereinafter referred to as simply “SunGard”) to utilize processors, storage, network components and sufficient resources to continue the critical functions NY-HX operations, in a manner consistent with eMedNY’s disaster preparedness. To ensure a timely recovery of the total hardware configuration, the Operating System files and critical data files will be backed up to storage units located at a SunGard disaster backup facility in Carlstadt, NJ. Data will be frequently updated at the recovery center to provide for a fast resumption of services should the primary site become disabled. As shown in Appendix F, a complete list of equipment to be located at the Carlstadt facility will be prepared as part of DR facility set up currently scheduled for November 2013.

3.1.2 Backups

All production guest system images will be backed up in their entirety once a week. The production databases that change daily will be backed up on a daily basis. Backups of the server images for both physical and virtual will be done via the NetBackup software. Production Database backups will be via a combination of synchronous data replication at the node level within the data center and asynchronous data replication to the SunGard facility. Replication of key production NY-HX servers that are virtualized will be replicated to the DR location as images via the Veeam image backup and replication software.

CSC will also back up the programs and data residing at SunGard in ancillary data center subsystems that are not connected to the Hitachi VSP storage system, on a routine schedule. These systems will be backed up on a regular basis so as to facilitate timely resumption of NY-HX functions in the event of a disaster at the primary site.

3.1.2.1 Operating System

Operating Systems will be backed up on the Hitachi VSP at SunGard using Veeam backup software. When the Operating Systems change at the primary site, the change will be reflected also at the backup site. In the event of activation of the hot site, CSC will activate the NY-HX servers via the guest images that were backed up to our backup storage.

3.1.2.2 Application Software

The critical application software will be backed up at the NY-HX site as part of the guest images, for non-java container applications, with the Veeam as well as written to the storage at SunGard. Java container applications will be replicated to the SunGard location via the Deployment Management software within the IBM WebSphere Application Server. A third copy will be written to portable media and stored offsite.

3.1.2.3 Data

Critical data files will be electronically copied via communication lines to SunGard; the database supporting the NY-HX will run on the Red Hat OS in a HA/DR multi-node configuration. All nodes are active. Data is replicated synchronously across 2 nodes local to the data center. Data is replicated asynchronously with the DR site.



3.1.3 Checkpoint/Restart Capabilities

Normal checkpoint/restart facilities are an integrated feature of NY-HX system. This feature minimizes lost time due to the interruption of processing by any cause. In addition, most of the online and batch portions of the system are transaction based using the DB2 COMMIT/ROLLBACK process. In the event of a production failure, this transaction-based system will allow processing to be restarted from the last completed transaction.

3.1.4 Offsite Storage and Retention

CSC maintains Operating System software images, application software images, and critical data at SunGard. In addition to this, copies of all files will be backed up and stored at Iron Mountain.

3.1.5 Help Desk

CSC Disaster preparedness for the NY-HX Enrollment Call Center operations will be completed by NYSDOH and/or Maximus, as that operations model is designed. CSC anticipates that NYSDOH and/or Maximus will identify primary and backup contacts to be named in CSC's DR plan, along with their emergency contact information, to allow both State and/or Maximus enrollment center operations to be re-directed to the Disaster site connectivity to NY-HX systems as appropriate to continue operations in the call center.

Technical or system related help desk calls, which are internal to CSC, will be routed to another CSC facility.

3.1.6 Documentation

All manuals necessary to support the operating systems and software will be available at SunGard in online readable format. Upon declaration of a disaster, the Iron Mountain courier will transport additional hard copy and CD-ROM formatted documentation for third party software to SunGard. User documentation, including operating instructions and balancing procedures, will be stored at Iron Mountain in electronic and hardcopy format and updated when necessary. Application system documentation will be stored at Iron Mountain in electronic format, and updated periodically.

3.1.7 Telecommunications

CSC has designed a network to provide for all NY-HX contractual requirements. Diagrams of connectivity to the DR environment will be updated in this document in Appendix K below, reflecting as-built conditions when those environments are defined in 2013.

Verizon, who is our local carrier, will redirect our local data and voice calls to our disaster recovery site as soon as possible.

3.2 Disaster Recovery Procedures

This section of our plan describes the procedures that would be used to recover from an actual disaster. These plans describe general procedures to be followed, allowing sufficient flexibility for on-the-spot determinations of the most effective way to address specific situations. Internal distribution of this plan will be to all persons who have either a direct or an advisory role in Disaster Recovery activities described in the plan. Procedures to be implemented in an actual disaster are indicated in Appendix H.

3.2.1 Assessment

The Account Executive, as part of the Management Team, will activate the Contingency Assessment Team. The Account Executive will notify and inform this team to convene at the NY-HX facility as soon as possible to evaluate the condition of the data center.

3.2.1.1 Team Meets and Assesses Site

The assessment team will assess the damage to facilities and determine which processes can still be accommodated within the facility and which must be relocated. They will determine what equipment if any is salvageable, and note that information on a checklist (Appendix D). Once that determination has been made, the team members responsible for the functions to be relocated will put their recovery plans



into operation. The team members will also assist with notification to subcontractors, suppliers, and vendors that a disaster has been declared and whether/how they will be affected.

3.2.1.2 Relocation Decisions Finalized and Implemented

Once the extent of damage to the primary data center has been determined, the CSC team will jointly decide with senior Department representatives on the extent to which relocation of functions will be necessary.

3.2.1.3 Notifications

As one of the initial tasks of the Management Team, a call will be placed to SunGard and Iron Mountain to put both vendors on alert.

Once a decision has been made to declare a disaster, the Management Team will notify SunGard of the extent of the emergency, and what facilities will be required. SunGard provides a National Emergency Hot Line (866) 722-1313 that is available 24 hours a day every day exclusively for this function. The declaration call to SunGard must be made by one of the people listed on the Disaster Declaration form that has been submitted to SunGard; CSC will review the data on this form on an annual basis to insure that the information provided to SunGard is accurate. A sample of the form is provided in Appendix A.

Iron Mountain will be notified and requested to deliver necessary backup materials to the recovery site. The data center's disaster recovery team will be activated and sent to the recovery site to initiate offsite recovery operations.

All CSC employees who work in one of these operations areas will be contacted by telephone and instructed on when and where to report for work.

Premium providers will also be notified of pertinent modifications to operating procedures. Team members will also assist with notification to subcontractors, suppliers, vendors and service bureaus that a disaster has been declared and whether/how they will be affected. Information for the media will be coordinated through a single CSC contact person, subject to Department approval.

3.2.2 Facilities and Staffing

The following sections describe the provisions CSC will be making to provide facilities and staff to continue NY-HX operations in the event of relocation to a disaster recovery site.

3.2.2.1 Location

Data center operations will be shifted to a SunGard facility, located at 777 Central Boulevard, Carlstadt, NJ, that can provide all required resources and services.

For the purposes of this plan, we are assuming that regular data center staff will be available to assume disaster recovery duties. This NY-HX plan will need to be augmented with detailed instruction that will enable staff other than the regular data center staff, to ensure its viability even in the instance when the regular staff would not be available.

Data center management has designated a complement of staff members to be members of the Disaster Recovery Team. The primary team is listed in Appendix C. This team will possess all necessary skills required to resume operations at the disaster recovery site. Once a disaster has been declared this team will immediately be sent to the disaster recovery site to work with the recovery site staff in performing all tasks required to restore critical system operations.



Additional staff members will then be transported to the disaster recovery site, to augment and relieve the initial group. The makeup of this group will depend on the extent of the emergency, and the estimated time necessary to restore operations at the primary site. Before departing for SunGard, an assessment will be made of the status of all production cycles, so that decisions can be made as to data restoration and the resumption of production processing.

3.2.2.2 Data Required

Critical data will be available at the disaster recovery site, due to the regular copying process. The hardware provided at the SunGard site will be listed in Appendix F when finalized.

Systems support personnel will utilize the current software vendor list to obtain any special codes that must be used to allow the system software to run at an alternate site. A list of all current software running for NY-HX will be listed in an appendix when as-built conditions are created in June 2013.

CSC will direct Iron Mountain to deliver whatever other data is necessary from their backup vaults. If production was interrupted in mid-cycle, some data may have to be reproduced by re-running certain job streams.

3.2.2.3 Backups

Once CSC starts to run production jobs from the SunGard site, we will need to resume daily and weekly backups as per normal schedules. These backups will be sent to an Iron Mountain facility close to the disaster recovery site, as a protection from a disaster of some kind at the backup site itself. Iron Mountain has two off-site storage facilities close to SunGard; one is located in Wood Ridge, NJ and another in New York City. During the time CSC would be using the disaster backup facilities, there will be no remote copies made of the data; all backups will be written to tape.

3.2.2.4 Communication Switchover

Verizon, as the local NY-HX communication provider, will redirect electronic communications to all necessary recovery sites as soon as possible. FTP data will be redirected to a network access server at SunGard for processing. Connectivity for these environments will be listed in an Appendix to this document based on as-built conditions.

3.2.2.5 Courier Services

CSC will arrange for Iron Mountain to provide couriers between the offsite storage facility and SunGard to affect backup material transfer. Iron Mountain will also provide courier service between the data center or command center and SunGard.

3.2.2.6 Facility Security

The SunGard facilities are fully secured environments for our use while they are needed. Security features include a 24-hour guard service, magnetic card access restrictions and the requirement of employee verification and badge services. No one will be allowed into the area that CSC is using for recovery without our permission. No cameras are allowed in the area.

3.3 Restoration Procedures

This section of our plan addresses the procedures that will be necessary to restore operations to the primary site.

3.3.1 Repair Primary Site

Once the Disaster Recovery plan has been implemented and operations have stabilized, the Assessment Team will initiate action to repair the damaged facility or relocate operations to another permanent facility that is suitable to house NY-HX production operations.

3.3.2 Restore Hardware

After the Assessment team has determined that a piece of equipment has been damaged, CSC will put in a rush order for a new piece of equipment. CSC has corporate-wide relationships with all of our chosen hardware vendors, and they are accustomed to responding to emergency situations. CSC will coordinate with the vendors and establish a delivery date to coordinate with when the building will be repaired

3.3.3 Restore Software

CSC will use NetBackup and Veeam software to replace the system software files back from the disaster recovery site to the repaired facility. The files that do not need to be urgently replaced will be loaded to tape and restored.

3.3.4 Move Data

After the operating systems and guest images are restored, the application files and java container applications will be restored. Once the primary site has been restored to operating condition, the network connections between the disaster recovery site and Columbia Turnpike will be re-established. Critical databases and data files will be copied back to the primary site via their designated replication method. This synchronization will ensure that an up-to-date copy of the critical files will be ready for transfer of operations back to the primary site. CSC will restore the current generation of non-critical data files from back-ups taken at the backup site.

3.3.5 Notification

The State will be notified of a date that production will resume at the original or replacement site. The Management Team will provide notification to the public and providers via the NY-HX Website, that the facility has been restored.

3.3.6 Switch Telecommunications

When our primary site is restored to operating order, Verizon will redirect our network to our primary location.

3.3.7 Relocate Staff

The staff will be transferred back to the repaired facility in stages for production resumption.

3.3.8 Resume Production in Primary Facility

Following the replacement, restoration, and/or loading of the necessary hardware, software and data files to the primary facility, testing will be performed to ensure that all systems are fully functional and there are no problems before operations are restarted. Connectivity with premium providers and other established interfaces. Production will resume at the primary facility following the successful completion of testing.

After we restore all system and data files and test the system we will begin running the less critical production job streams first to ensure there are no problems before we restart the most critical applications. Upon successful completion of these initial non-critical jobs, CSC will begin transitioning additional jobs to the new environment until full production has been achieved.

3.4 Disaster Preparedness Testing

CSC's disaster preparedness will be tested periodically to assure readiness for an actual emergency. We will work closely with the State to plan for and conduct the tests.

CSC policy states that Disaster Recovery plans must be reviewed at least annually. At that time, the disaster declaration data will be reviewed for accuracy. Escalation/call lists will be verified for accuracy on a quarterly basis. Semi-annually, alternate recovery contracts will be reviewed to insure they cover the current capacity required for a full recovery. In addition, off-site tapes and related procedures will be semi-annually audited to insure that all tapes/information needed for a timely recovery are kept in a secure facility and are available to be shipped to any alternate facility.

3.4.1 Scope of Testing

CSC and the State will jointly decide the applications to be tested, data volumes, and duration of tests. The Office of the State Comptroller (OSC) production applications will also be tested and OSC staff will participate in the planning for the testing of these applications.

3.4.2 Location of Test

The tests will take place at SunGard's Carlstadt, NJ facility.

3.4.3 Testing Procedures

After the scope of testing has been determined, procedures for the actual tests will be developed and approved by the State. Tests will then be executed according to the agreed-to procedures, and results will be evaluated against predetermined standards.

3.4.4 NYS Review of Test Results

A debriefing meeting will be set up with New York State and OSC representatives after the test to review the results.



Appendix A – Management Team (MT)

State of New York Department of Health Contacts

	Name	Office Telephone	Mobile Telephone
Contract Administrator	Christine Hall-Finney – Division Director	518-257-4481	518-573-4940
Alternate 1	Dennis Wright	518-649-4274	
Alternate 2			

State of New York Office of the State Comptroller

	Name	Office Telephone	Mobile Telephone	Home Telephone
	Warren Fitzgerald State Government Accountability	518-402-0495 518-474-3271 (Alt)	518-527-8561 (Pers)	518-783-6403
Alternate 1	Andrea Inman State Government Accountability	518-402-0590 518-474-3271 (Alt)	None	518-479-7041
Alternate 2	Gail Gorski State Government Accountability	518-402-0182 518-474-3271 (Alt)	518-312-2561 (Pers)	518-272-3401

Management Authorized to Declare a Contingency

	Name	Office Telephone	Mobile Telephone	Home Telephone
NY Account Executive	John Caterham	518-257-4800	518-867-7917	518-326-3578
Back-up	Mark Simonsen	518-257-4805	518-527-1386	518-426-0064
Back-up	Steven Rubenstein	518-257-4354	518-669-9510	518-669-9510
Back-up	John Moran	518-257-4406	314-440-0223	314-440-0223

Each of the people listed above has confidential instructions on how to declare a contingency. Their names have been submitted to SunGard on a form like the one show below.

CSC Management Team Responsibilities Lists

Pre-contingency Responsibilities

1. Review and approve results of periodic Data Center Recovery Plan maintenance updates.
2. Know and understand the procedures for notifying the SUNGARD Disaster Recovery Services of a contingency situation that requires moving the data center operations to the disaster recovery site.
3. Periodic review and maintenance of the data center and vault personnel requirement's list.
4. Periodic audit of the offsite storage vault, inventory vault contents, and verification that all required materials are being sent offsite.
5. Periodic review of the SunGard's Disaster Recovery Services contract
6. Review and approve results of periodic disaster recovery tests.
7. Periodic review of departmental business continuity plans.

Contingency Responsibilities

1. Activate the Contingency Assessment Team
2. Inform State of NY, Dept of Health of the situation.
3. Alert Iron Mountain of the potential for declaring a contingency.
4. Alert SunGard of the potential contingency declaration
5. Based on the recommendation from the Contingency Assessment Team, decide jointly with the Department of Health whether to invoke the Data Center Recovery Plan.
6. Formally notify State of NY Dept. of Health.
7. Contact SunGard to declare a data center contingency.
8. Inform Iron Mountain of the contingency declaration.
9. Provide overall leadership to the personnel performing the data center recovery.
10. Contact all the Disaster Recovery team managers to assemble their personnel to perform data center recovery at SunGard.
11. Contact and authorize the Operations/Tape Library Team to request offsite storage to send materials to the SunGard's data center recovery facility in Carlstadt, NJ
12. Contact the software product vendors to facilitate use of software licenses at the disaster recovery site, which has been prearranged.
13. Inform SunGard of the arrival times and number of people traveling to the Carlstadt, NJ location.
14. Provide transportation to the data center disaster recovery site.
15. Arrange lodging at the data center disaster recovery site.

Post-contingency Responsibilities

1. Assess the overall performance of teams during the recovery process.
2. Assess the overall effectiveness of the Data Center Recovery Plan.
3. Assess the overall effectiveness of SunGard.
4. Advise the recovery teams of migration date to the primary facility.
5. Based on the availability of the data center personnel, make recommendations for updates to the Human Resource Plan.



DISASTER DECLARATION AUTHORIZATION / CUSTOMER PROFILE

SECTION I - CUSTOMER PROFILE INFORMATION

SUBSCRIBER NAME: _____

ADDRESS: _____

CONTRACT #: _____

AUTHORIZATION CODE: _____

PRIMARY PRODUCT: _____

LAST DDA UPDATE: _____

PRIMARY OPERATIONS CONTACT: (If authorized to declare a disaster, also include this contact in Section II of this form)

NAME: _____

TITLE: _____

ADDRESS: _____

PHONES: (Cellular, Fax, Home, Pager, Work)

_____ (____) _____ - _____ EXT/PIN. _____

SECTION II- DECLARATION AUTHORIZATION

NAME: _____

TITLE: _____

ADDRESS: _____

PHONES: (Cellular, Fax, Home, Pager, Work)

_____ (____) _____ - _____ EXT/PIN. _____

PERSONAL DDA CODE: _____

PRIMARY CONTACT TO DECLARE DISASTER: _____ (YES/NO)



Appendix B – Contingency Assessment Team

	Name	Functional Responsibility	Office Telephone	Mobile Telephone	Home Telephone
NY-HX Team Leader:	John Moran	Program Director	518-257-4406	314-440-0223	314-440-0223
NY-HX Alternate Leader:	Tom Silvius	Solution Director	518-257-4730	518-469-8947	518-731-8048
NY-HX Team Member:	Paulot Truchard	Enterprise Architect	518-257-4755	518-428-1679	518-428-1679
NY-HX Team Member:	Mark Simonsen	Contracts	518-257-4805	518-527-1386	518-426-0064
NY-HX Team Member:	Russell Ralbovsky	Development Manager			
NY-HX Team Member:	Carlton Brown	Facilities Manager	518-257-4600	518-441-4625	518-434-0942
ITIS Team Leader:	Michael McKinney	Service Delivery Manager			
ITIS Team Member:	Belinda Losowski	CSS Engineering Manager (Wintel/LAN, Mainframe, Ops)	518-257-4210	518-368-9494	518-784-3878
ITIS Team Member:	William Peacock	Manager Solutions Architecture	518-257-4277	518-423-3771	518-377-7483
ITIS Team Member:	Vince Meleco	Manager Network Engineering	518-257-4353	518-248-9755	518-432-3997
ITIS Team Member:	Dave Richardson	Computer Operations Manager	518-257-4414	518-421-3242	518-273-6739
ITIS Team Member:	Scott Miles	EUSS Lead (Field Services)	518-257-4224	518-859-0929	518-598-1007
ITIS Team Member:	James Murray	IT IS Project Manager	518-257-4153	518-368-7158	864-553-6389
ITIS Team Member:	David Dobert	GSS & Information Security Lead	518-257-4285	518-423-7576	518-674-3347
Non-CSC Team Member:	Joe LaMattina	OptumInsight Representative	518-257-4197	603-553-7570	603-659-5467
Non-CSC Team Member:	Eli Soto	Maximus – Call Center Representative			



Contingency Assessment Team Responsibilities List

Pre-contingency Responsibilities

- | |
|---|
| <ol style="list-style-type: none">1. Understand the conditions/criteria that constitute a contingency situation.2. Understand the process for declaring a contingency. |
|---|

Contingency Responsibilities

- | |
|---|
| <ol style="list-style-type: none">1. The Assessment Team Leader will contact and assemble the personnel to assess the situation.2. Inform the Management Team of the situation.3. Advise the Management Team on the course of action to be taken. |
|---|

Post-contingency Responsibilities

- | |
|---|
| <ol style="list-style-type: none">1. Manage restoration of primary facility or relocation to alternate facility.2. Determine when primary facility or alternate facility is available to use.3. Coordinate with Disaster Recovery team relocation into primary or alternate facility. |
|---|



Appendix C– CSC Disaster Recovery Operations Team (DR)

	Name	Functional Responsibility	Office Telephone	Mobile Telephone	Home Telephone
Contingency Services Analyst	Mary Snyder	Disaster Recovery coordinator	330-651-2189	330-651-2189	330-793-0290
Contingency Services Analyst		Alternate Disaster Recovery coordinator	817-821-5719	817-821-5719	817-431-1476
Network Team Member	Vince Meleco	Manager Network Engineering	518-257-4353	518-248-9735	518-432-3997
Operations Team Member	David Richardson	Computer Operations Manager	518-257-4414	518-421-3242	518-273-6739
Operations Team Member	Sharon King	Lead – Scheduling, Automation, Application Mgmt	518-257-4785	518-441-2693 877-635-9844 (pager)	518-346-4770
Operations Team Member	Dan Rivera	Lead – RDC Data Center	518-257-4215	518-248-0836 877- 288-6572 (pager)	518-542-3466
Technical Services Team Member	William Peacock	Manager Solutions Architecture	518-257-4277	518-423-3771	518-377-7483
Storage and Tape Management Team Member	Kris Henrikson	Storage Administrator	207-442-5089	207-720-0535	
Storage and Tape Management Team Member	Kristie Reid	Storage Administrator	412-374-3626	888-245-8382	412-422-8887
Data Security Team Member	Dave Dobert	Information Security Leader	518-257-4285	518-423-7576	518-674-3347
Data Base Team Member	Diane Uhl	Senior Database Administrator	817-762-8772	817-313-1112	817-613-0553
Systems Software Support Member	Belinda Losowski	CSS Engineering Manager	518-257-4210	518-368-9494	518-784-3878
Systems Software Support Member	Rob Irizarry	Lead – Wintel	518-257-4399	518-894-5848	
Network Software Team Member	Brian Phillips	Mainframe Network Services	817-762-8075		817-370-2498
Systems Software Support Member	Gladys Behnke	MVS Client Team Lead	860-664-1780	860-581-0017	860-669-6126



CSC Disaster Recovery Operations Team Responsibilities List

Pre-contingency Responsibilities

1. Develop a network configuration to support the NY-HX operations during a contingency situation.
2. Keep the contingency network definitions current.
3. Maintain and understand the network recovery procedures and configurations.
4. Test the contingency network (support recovery testing).
5. Maintain system pack backups.
6. Maintain system catalog backups.
7. Ensure all critical data is mirrored to the disaster backup site location.
8. Maintain a copy of daily operating procedures offsite.
9. Be knowledgeable of all backup and recovery procedures.
10. Ensure system software documentation and recovery procedures are maintained (Procedures, I/O configuration, recovery jobs, etc.)
11. Test the system recovery procedures (support recovery testing).
12. Maintain documentation on data base recovery procedures.
13. Ensure the application data is either being remote copied or backed up regularly and meets the recovery strategy.
14. Review the Data Center Recovery Plan on a regular basis.
15. Audit the plan to ensure information is current.
16. Schedule periodic tests with SunGard.
17. Coordinate pre-test planning activities.
18. Document test results.

Contingency Responsibilities

1. CSM - Provide primary coordination of all recovery activities.
2. Coordinate with SDM on assessment of personnel availability.
3. Restore system and connectivity to State of NY Dept of Health and system users.
4. Maintain an operational environment at the disaster recovery site until primary or alternate facility available.

Post-contingency Responsibilities

1. Coordinate with Disaster Recovery team relocation into primary or alternate facility.
2. Assess system performance in recovery mode and the overall effectiveness of the Data Center Recovery plan and make recommendations.



Appendix D – Assessment Charts

MAJOR SYSTEM COMPONENTS	CSC Functional Area	Vendor Assisting/ Directing assessment	Not Affected	Damaged	Unsure	Fixable
Mainframe	Operations					
Channel Extenders	Operations					
Hitachi VSP	Operations					
SAN Switches	Operations					
Backup System	Operations					
IBM xSeries Systems	Operations					
SCSI Connections	Operations					
DLT 7000 Tape Drives	Operations					
Administrative Workstation	Operations					
Reel Librarian (robotic archiving system)	Operations					
Cisco Routers	NES					
Network Connectivity	NES					
LAN/WAN	LAN/Server					
PBX	NES					
Telephone System	NES					



WORK AREA COMPONENTS	CSC Functional Area	Vendor Assisting/ Directing Assessment	Not Affected	Damaged	Unsure	Fixable
Office Areas	Facilities Data Capture Dept	N/A				
Production Control	Production Operations					
Data Control	Production Operations					
Tape Library	Production Operations					
Furniture and Supplies	Facilities Production Operations					



WORK IN PROCESS	CSC Functional Area	Vendor Assisting/ Directing Assessment	Not Affected	Damaged	Unsure	Fixable
Financial Management	Application Layer					
Plan Management	Application Layer					
Customer Service Center	Content Management Presentation/Access Layer					
Fax System	Content Management Presentation/Access Layer					
Content Repository	Data Layer					
Data Warehouse/Reporting	Data Layer					
Master Data	Data Layer					
Transactional Data	Data Layer					
Eligibility/ Subsidy Determination	Eligibility and Enrollment Application Layer					
Enrollment	Eligibility and Enrollment Application Layer					
Quoting Engine	Eligibility and Enrollment Application Layer					
Metadata Files	Production/ Operations					
Email/ Messaging	Search Engine Presentation/Access Layer					
Telephony	Search Engine Presentation/Access Layer					
Web Portal	Search Engine Presentation/Access Layer					
Enterprise Service Bus/BPM/BPEL/Orchestration	Service Layer					
Identity Management and Security Admin.	Service Layer					



Rules Engine	Service Layer					
---------------------	---------------	--	--	--	--	--



FACILITY COMPONENTS	CSC Functional Area	Vendor Assisting/ Directing Assessment	Not Affected	Damaged	Unsure	Fixable
Structural Condition	Facilities					
Security Stations	Facilities					
Water	Facilities					
Gas/Electric	Facilities					
Air Conditioning	Facilities					
UPS	Facilities					
Diesel Generator	Facilities					
Walls	Facilities					
Floors	Facilities					
Ceilings	Facilities					
Detection/ Suppressant System	Facilities					
Electrical Equipment	Facilities					



Appendix E – Preliminary Vendor List

Vendor	Area/Contact	Telephone/Account Info
321 Gang	Tony Scafidi	603-860-8374
Adaptive	James Bedford	978.994.6551
Active Risk Inc.	Karl Pringle	703-909-9325
ASG (Allen Systems Group)	ASG Support	800-354-3578
Document Direct		800-242-2121
Avaya (Phone vendor)	Avaya Help Desk	#0003119888
CDW Computer Centers, Inc	Jake Jensen	703-262-8119
CISCO	Cisco Tac Procurement: Carter Yepsen	1-800-533-2447 518-472-5230
Computer Associates	Technical Support OPSMVS Support	412-494-1341 412-494-1302 site id 222974 pin 30
Dell	Derek Trawick	512-513-9905
Emergent	Danny Climo	703-584-4560
Fire Department		911
Generator Vendor	See Kinsley Power	
Hart Alarm Systems	Steve Hart	518-272-2007
hCentive	Eric Letada	800-984-7952
Hitachi/Brocade	Bill Ryan Procurement: Kathy Renner	781-593-2666 763-268-6140
Hitachi Data Systems (HDS)	Doug Kryszak	904-745-7801 #R018769
IBM (Account Rep)	Zari Tabatabai	914-642-4865
IBM (Service Desk)	IBM Customer Number is: 2444363 Contract Number is: CFTPQKL Contract Start Date is: 10/01/2003 Purchase Order Number is: 101020 Procurement Contact: Lisa Ramos	800-426-7378 (800.IBM.SERV) 800-426-1757 x3651
IBM (Mainframe)	Grant Perkins Procurement: Sherri Penn	804-327-4541 410-332-2573 #2064801
IBM (LAN/Server)	Jerry Bennett	904-928-4548
Insight Public Sector Inc Software	Noel Amendson	800-859-4906
Intel Americas	Katrina Kehlet	410-263-3616



Vendor	Area/Contact	Telephone/Account Info
Iron Mountain	Rose West	518-828-8958
Johnson Controls		800-274-4524
Johnson Controls (A/C)	Procurement: Dan Keating	518-869-9595
Kinsley Power Systems	Joseph Pugliese	518-458-8614
Lynn Associates	Bob Lynn	518-459-1239
Microsoft	Customer Support	800-936-3100 Access # 001482632
OptumInsight	Joe Lamattina	518-257-4197 603-659-5497
PBX vendor	See Avaya	
Police Department		911
Physical Security	See Hart Alarm	
Rensselaer Post Office	Frank Renasiewicz	518-449-5012
Sprinkler system	See Hart Alarm	
SunGard ARS	Janine Morgan Procurement: Mike Matlarn	610-205-3639 703-326-4983
Oracle	Jason Weiss	518-782-1020
Ricoh	Claudine Crljen	562.597.4294
Symantec	Enterprise Support	800-927-4017
TW Telecom	Susan Burton	518-640-0908
UPS Vendor	See Lynn Associates	
Wright - Line	Jo Ann Schjorring	518-945-3121
Vanguard Integrity Professional Customer Support	Cust. Support	702-792-0014
Verizon	Data/Voice Communications	518-890-7711 #518M566359
VMware	Support Account Debbie Guditus	650-475-5322
Zoho	Ken Smith	925-924-9500



Appendix F – Disaster Recovery Site Configuration List

Located in the Carlstadt, NJ facility, the following sheet will be used to inventory the equipment when it is deployed to the facility in November 2013:

QUANTITY	MODEL	DESCRIPTION

Appendix G – Implementation Plan

The Implementation Plan is very straightforward in that it identifies tasks required to be completed once an incident has occurred. The ID sequence number is in the first column; the predecessor column (second column) identifies which task or tasks must precede this task. The task name/description in the third column, with duration, projected start and end times in columns four through six. An area for notes completes the table.

ID	PRED	TASK NAME	DURATION	START TIME	FINISH TIME	NOTES
----	------	-----------	----------	------------	-------------	-------

The following is a table of potential team resources that could be used during the recovery.

Code	Resources
AP	Applications Team
AR	Iron Mountain Tape Vault Vendor
AT	Contingency Assessment Team
BC	Business Continuity Team
CS	Data Center Recovery Plan Coordinator
DB	Data Base Team
DC	Data Capture Team
DS	Data Security Team
DW	Data Warehouse Team
LA	LAN Team
MT	Management Team
NT	Network Team
OP	Operations Team
PC	Production Control
RC	SunGard Recovery Center Team
RT	Disaster Recovery Team (in general)
TS	MF Technical Services Team
UN	UNIX Team

The Implementation Plan is a 'script' for executing the overall recovery plan. It is intended to drive multiple teams performing tasks concurrently to achieve a faster recovery.



The Projected Start time is 00:00 (hour:minute). The Projected Complete time minus the Projected Start time is the estimated duration for the task. Tasks that are support in nature do not have projected times; they will have N/A (Not Applicable) or No Time in the projected time columns.

Task Charts

The following is a listing of the tasks required to perform the recovery.

Contingency Assessment at the NY-HX Facility

ID	PRED	TASK NAME/DESCRIPTION	DURATION	START TIME	FINISH TIME	NOTES
		Some contingency situation occurred.		00:00	00:00	
MT01		Activate the Contingency Assessment Team.		00:00	02:00	
MT02	MT01	Inform Department of Health senior managers of the situation.		00:15	00:30	
MT03	MT02	Alert Iron Mountain of the potential of declaring a disaster.		03:00	03:15	
MT04	MT03	Alert the SunGard of the potential of declaring a disaster.		03:15	03:30	
MT04.1	MT03	Alert Maximus of the potential of declaring a disaster		03:30	03:45	
AT01	MT01	The Assessment Team Leader will contact and assemble the personnel to assess the situation.		02:00	03:00	
AT02	AT01	Inform the Management Team of the situation.		03:00	04:00	
AT03	AT02	Advise the Management Team on the course of action to be taken.		04:00	05:00	
MT05	AT03	Based on the recommendation from the Contingency Assessment Team, jointly decide with State management whether to invoke the Data Center Recovery Plan.		05:00	05:30	
MT06	MT05	Inform the Department of Health senior managers of the decision.		05:30	06:00	

Notify/Activate Personnel

ID	PRED	TASK NAME/DESCRIPTION	DURATION	START TIME	FINISH TIME	NOTES
MT07	MT06	Contact Iron Mountain to declare a disaster.		05:30	05:45	
MT08	MT07	Contact SunGard to declare a disaster.		05:45	06:00	
MT08.1	MT08	Contact Maximus to declare a disaster		06:00	06:15	
MT09	MT08	Provide overall leadership to the personnel performing the data center recovery.		N/A	N/A	
MT10	MT09	Contact all the team managers to assemble the personnel to perform the data center recovery at SunGard.		06:00	06:30	
CS01	MT10	The Data Center Recovery Plan Coordinator Team manager will assess personnel availability and assign personnel to assist the data center recovery.		06:30	07:30	
CS02	CS01	Provide primary coordination of all the recovery activities.		N/A	N/A	
NT01	MT10	The Network Team manager will assess personnel availability and assign personnel to assist the network recovery.		07:30	08:30	
NT02	NT01	Notify AT&T to reroute the network.		08:30	09:30	
OP01	MT10	The Operations Team manager will assess personnel availability and assign personnel to assist the data center recovery.		07:30	08:30	
MT11	OP01	Contact and authorize the Operations Team to request offsite storage to send materials to SunGard.		08:30	09:30	

ID	PRED	TASK NAME/DESCRIPTION	DURATION	START TIME	FINISH TIME	NOTES
TS01	MT10	The MF Technical Team manager will assess personnel availability and assign personnel to assist the data center recovery.		07:30	08:30	
LA01	MT10	The LAN Team manager will assess personnel availability and assign personnel to assist the data center recovery.		07:30	08:30	
UN01	MT10	The Mid-Range Team manager will assess personnel availability and assign personnel to assist the data center recovery.		07:30	08:30	
PC01	MT10	The Production Control Team manager will assess personnel availability and assign personnel to assist the data center recovery.		07:30	08:30	
DB01	MT10	The Data Base Team manager will assess personnel availability and assign personnel to assist the data center recovery.		07:30	08:30	
AP01	MT10	The Application Team manager will assess personnel availability and assign personnel to assist the data center recovery.		07:30	08:30	
DS01	MT10	The Data Security Team manager will assess personnel availability.		07:30	08:30	
MT12	MT10	Contact software product vendors to obtain licenses and manuals if necessary.		07:30	09:30	
MT13	MT10	Contact Hotel providing command center facilities to reserve space.		07:30	08:00	

Employees/Materials to SunGard and the Command Center

ID	PRED	TASK NAME/DESCRIPTION	DURATION	START TIME	FINISH TIME	NOTES
----	------	-----------------------	----------	------------	-------------	-------

ID	PRED	TASK NAME/DESCRIPTION	DURATION	START TIME	FINISH TIME	NOTES
OP02	MT11	Contact Iron Mountain with shipping instructions for back-up tapes, reports, and manuals.		09:30	9:45	
OP03	OP02	Obtain estimated time of arrival (ETA) of off-site material at SunGard.		10:00	10:15	
OP04	OP03	Inform SunGard of the ETA for back-up tapes, reports and manuals.		10:15	10:30	
MT14	CS01	Inform SunGard/Command Center of the arrival time and number of people.		9:30	10:00	
MT15	MT14	Provide road maps and directions to the SunGard facility in Carlstadt, NJ.		10:00	10:15	
MT16	MT15	Provide transportation to SunGard for people. (optional)		N/A	N/A	
MT17	MT16	Arrange lodging and personal expenses at the SunGard/Command Center site. (optional)		N/A	N/A	

Iron Mountain Prepares Shipment to SunGard Carlstadt

ID	PRED	TASK NAME/DESCRIPTION	DURATION	START TIME	FINISH TIME	NOTES
AR01	MT03	Obtain tape pull list report.		03:15	03:45	
AR02	MT07	Pull tapes and box for shipment.		05:45	9:45	
AR03	OP02	Confirm SunGard Ship To addresses.		9:45	10:00	
AR04	AR03	Send off-site material.		10:00	10:15	

Activities at the SunGard Business Recovery Services Centers

ID	PRED	TASK NAME/DESCRIPTION	DURATION	START TIME	FINISH TIME	NOTES
RC01	MT04	SunGard alerts the duty team.		03:30	03:45	
RC02	MT08	SunGard contacts the customer with specific recovery location (CCC) information.		06:00	6:30	
RC03	RC02	SUNGARD prepares the system and network configuration according to the contract.		06:30	10:30	
RC04	AR04	SunGard receives off-site material delivered by Iron Mountain		12:30	13:00	
RC05	RC03	Disconnect Gig-E lines between Rensselaer and Carlstadt, if necessary.		6:30	7:00	
RC06	RC02-RC05	Redirect Hitachi VSP through the data switch to hardware being used in the recovery		10:30	11:30	

Teams Travel to the SunGard/Command Center

ID	PRED	TASK NAME/DESCRIPTION	DURATION	START TIME	FINISH TIME	NOTES
RT01	MT14	All personnel identified by the team managers to assist with the data center recovery get ready to travel to SunGard/Command Center.		8:30	9:45	
RT02	RT01	All personnel identified by the team managers to assist with the data center recovery arrive at the SunGard.		12:00	13:00	
RT03	RT01	All personnel identified by the team managers to assist with Provider Inquiry and Disaster Management arrive at the Command Center.		9:45	11:00	

Setup/Restore at the SunGard/Command Center

ID	PRED	TASK NAME/DESCRIPTION	DURATION	START TIME	FINISH TIME	NOTES
OP05	RC04 RT02	Inventory materials received from Iron Mountain.		13:00	17:00	
OP06	OP05	Build and populate the tape library at SunGard.		17:00	19:00	
OP07	OP06	Clean the tape drives.		19:00	19:15	
OP08	OP07	Ensure a master console and terminals are available.		19:15	19:30	
OP09- CS03 - LA02 - UN02	RT02	Inspect the SunGard Operations Suite to ensure the setup is correct. (i.e., telephones, workstations, printers)		13:00	16:00	
MT18	RT03	Inspect the Command Center Facility to ensure the setup is correct. (i.e., telephones, workstations, printers)		11:00	12:00	
TS02	RT02	Review the hardware/network configuration to ensure all device addresses and types are correct.		13:00	14:00	
OP10	RT02	Ensure the tape drives and replicated data storage are on-line and available.		13:00	13:15	
OP11	OP09	Ensure operations documentation and system manuals are available.		13:00	13:30	
RT04	OP11	Review all applicable recovery procedures and checklists.		13:30	14:30	
RT05	OP11	Review all recovery tasks before initiating recovery.		13:30	14:30	

Restore Operating System/Applications

ID	PRED	TASK NAME/DESCRIPTION	DURATION	START TIME	FINISH TIME	NOTES
TS03	OP11-RT02	IPL mainframe pointing to alternate IOCDS (Applies to DDO Phase).		16:00	17:00	
TS04	MT12	Apply zaaps obtained from vendors required to run on an alternate processor.		17:00	19:00	
TS05	TS04	ReIPL mainframe, if necessary.		N/A	N/A	
TS06	TS05	Initialize and configure any shared VSP volumes being used for the recovery.		19:00	21:00	
TS07	TS06	Restore Linux Partitioning and VMWare Guests		N/A	N/A	
TS08	OP04	Assist with restoration of critical applications.		N/A	N/A	
LA03	RT02	Insure connectivity between VMware systems is correct.		16:00	20:00	
AP07	AP06	Validate system security.		20:00	21:00	
AP08	AP07	Verify application access.		21:00	22:00	

Restore Network at the SunGard/Command Center

ID	PRED	TASK NAME/DESCRIPTION	DURATION	START TIME	FINISH TIME	NOTES
NT03	RC02-RT02	Ensure the network configuration provided by SunGard matches the contract specifications.		13:00	15:00	
NT04	NT03	Verify Call Center Access to NY-HX applications.		15:00	16:00	
NT05	NT04	Establish data communications to remote sites.		20:00	21:00	
NT06	NT05	Assist with network problem determination.		21:00	22:00	

Normal Operations setup at SUNGARD

ID	PRED	TASK NAME/DESCRIPTION	DURATION	START TIME	FINISH TIME	NOTES
TS08	TS07	Provide technical support to application programming staff, i.e. hands-on technical support for z/Linux, xSeries and VM component failures and problems.		N/A	N/A	
DS02	ST04	Resolve security related problems if necessary.		N/A	N/A	
OP12	OP10	Create scratch tapes for production use.		N/A	N/A	
OP13	OP11	Arrange for offsite storage for the backup tapes while operating at the SunGard.		N/A	N/A	
TS09	TS08	Establish a backup process in preparation for migration to the cold site or permanent location		N/A	N/A	
DB07	DB06	Assist the application users with the application data recovery.		N/A	N/A	
RC07	RC06	Provide 7x24 support for recovery		N/A	N/A	
CS04	CS03	Provide overall management for personnel at SunGard		N/A	N/A	
MT19	MT18	Provide overall management for personnel at command center		N/A	N/A	



Appendix H – Disaster Recovery Site Connectivity

This section will be completed when the NY-HX Physical Technology Model is documented in June 2013.



Appendix I – NY-HX Data Center Configurations

This section will be completed when Data Center Configurations are created in June 2013.