



**Exhibit to Data Center Services
Service Component Provider
Master Services Agreement
DIR Contract No. DIR-DCS-SCP-MSA-003**

Between

**The State of Texas, acting by and through
the Texas Department of Information Resources**

and

Xerox Corporation

**Exhibit 16
IT Service Continuity Management**

January 23, 2012

TABLE OF CONTENTS

1.0	INTRODUCTION.....	3
2.0	GENERAL DISASTER RECOVERY	4
2.1	Disaster Recovery Plan (DRP).....	4
2.2	Disaster Recovery Testing	5
2.2.1	Disaster Recovery Testing for Server and Mainframe Services	6
2.2.2	Disaster Recovery Testing for Email Services.....	6
2.2.3	Disaster Recovery Testing for Consolidated Data Centers	6
3.0	TRUE-UP OF INITIAL RTO LEVELS	7
4.0	SERVER SERVICE TIER RTO	7
4.1	Disaster Recovery Level Application Requirements	8
5.0	DISASTER RECOVERY FOR UTILITY SERVERS	9
5.1	Utility Server Email / Directory Services	10
5.2	Utility Server File / Print.....	10
6.0	OTHER CONSIDERATIONS.....	10
6.1	Texas Emergency Management Council	11
7.0	ADDITIONAL REFERENCES.....	11

EXHIBIT 16
IT SERVICE CONTINUITY MANAGEMENT

Update Methodologies and Attachments to Exhibit 16

The following update methodologies and attachment are incorporated as part of **Exhibit 16**:

Title	Methodology for Updating Associated Exhibit Attachment
<u>Exhibit 16</u> IT Service Continuity Management	<u>Exhibit 16</u> may only be modified by formal amendment, in accordance with <u>Section 21.7</u> of the MSA.
<u>Attachment 16-A</u> Disaster Recovery Plan	<u>Attachment 16-A</u> may only be modified by formal amendment, in accordance with <u>Section 21.7</u> of the MSA. Disaster Recovery Plans reside on the Portal. On-going development of the Disaster Recovery Plans is done in accordance with Section 2.4.11 of the Service Management Manual.

1. INTRODUCTION

Upon the occurrence of a disaster under the applicable Disaster Recovery Plans (DRPs), Service Provider shall promptly provide DR Services, including as described in and in accordance with the requirements of this Exhibit. In addition, this Exhibit sets forth certain requirements that Service Provider shall comply with in developing, maintaining and implementing DRPs.

2. GENERAL DISASTER RECOVERY

Texas has been pursuing a DR strategy based on having dual data centers to provide DR capabilities for each other. The highest levels of recovery are based on the use of the alternate Consolidated Data Center, and should be architected to meet the RTO of Applications through appropriate replication and storage of data.

1. Service Provider will be responsible for providing the resources, including network connectivity between the Consolidated Data Centers, and to such disaster location facilities needed to support its disaster recovery strategy.
2. Service Provider will work with DIR to establish declaration procedures and document those procedures in the Service Management Manual.
3. Service Provider shall assume all Third Party Disaster Recovery contracts in existence at the Commencement Date, and continue to utilize such contracts until such time that a successful test has been achieved for alternative solutions.
4. For IBM mainframes, the Service Provider shall implement a DR strategy within both Consolidated Data Centers which includes processor recovery via capacity back up (CBU) capabilities, data replication for Applications designated as having D0 RTO, and all necessary network, coupling facilities and channel resources required to meet the RTO.
5. The HHSC- E Unisys mainframe in the ADC shall be recovered using the HHSC – E Unisys mainframe in the SDC. In the event of a disaster or primary ADC system failure, the SDC mainframe shall be re-configured to assume operations of the ADC production workload. During this time, the development and test environments are replaced by this production environment. Disk data (DASD) will be recovered from either the replicated virtual tapes or physical tape media stored at an offsite location to within 24 hours (RPO) of the failure.

2.1 Disaster Recovery Plan (DRP)

1. Service Provider shall develop, maintain and implement a comprehensive DRP for Services provided to DIR Customers and in relation to any DIR Customer-specific DRPs, in each case subject to the DIR Customer's prior review and approval.
2. DRPs shall include the DIR Customer-specific plan and the Technical Recovery Guide for each of the DIR Customer's Applications.
3. For all Applications, within three (3) months after the Commencement Date, Service Provider shall update all existing DIR Customer-specific DRPs to reflect all changes implemented during the performance of Transition Services.

4. Such DRPs shall be updated at least once each quarter to reflect all changes implemented over the course of Service Provider's performance of the Services. Technical Recovery Guides shall be updated whenever a change is made to the environment or Application.
5. Updated DRPs (and Technical Recovery Guides) shall be sent for the applicable DIR Customer's review, and must document and demonstrate Service Provider's plan and capability to restore Applications within their applicable RTOs.
6. Service Provider will adjust the applicable DRPs whenever a DIR Customer's needs and use of the Services change.
7. DRPs shall contain the sections as outlined in **Attachment 16-A**, including Technical Recovery Guides.
8. All DRPs that are developed by Service Provider shall comply with all DIR Standards, including the National Institute of Standards and Technology Special Publication 800-34 and 800-66 Section 4.7, and shall be tested at least annually in accordance with applicable Laws.

2.2 Disaster Recovery Testing

1. Service Provider will assume the DR test schedules in existence at the Commencement Date, and work with DIR Customers to ensure that the DIR Customer annual test schedules continue without disruption.
2. In cooperation with DIR Customers, Service Provider will establish and schedule reasonable windows to accomplish all DR testing for that DIR Customer's Applications as documented in the Service Provider's annual DR test plan and schedule, in accordance with **Attachment 3-C**.
3. Service Provider will assist DIR and the appropriate governance committee, as specified in **Exhibit 6**, in prioritizing the test schedule of DIR Customer Applications.
4. Service Provider will actively engage DIR Customers in planning and preparation for annual test activities; including setting the objectives of the test.
5. Each such test shall address the specific needs of each DIR Customer (e.g. split-window testing, preparation testing prior to an annual test, off-site tape location review and reconciliation, etc.) The Service Provider's test execution must demonstrate, at a minimum, the Service Provider's ability to meet or exceed the designated RTOs for those Applications in the event of a disaster.
6. Service Provider shall, in conjunction with DR tests, include the associated Mainframe and/or Servers, as required to meet the objectives of the test.
7. Service Provider shall conduct all testing activities in such a manner so that active production, test, and development environments are not affected.
8. Service Provider shall notify DIR and DIR Customers of any anticipated DR risks, in accordance with Risk Management, where a DIR Customer may choose not to participate in testing.
9. Service Provider shall evaluate the results of the test and identify potential corrective actions. Service Provider shall provide initial test results to the DIR Customer and incorporate DIR Customer feedback into the final test results report.

10. Service Provider will facilitate test result review sessions with the DIR Customer to gain consensus on the success level of the test (e.g. successful, successful with issues, unsuccessful, etc.) and to identify corrective actions.
11. Service Provider will implement and track corrective actions until resolved

2.2.1 Disaster Recovery Testing for Server and Mainframe Services

1. All Mainframe and Server Applications will adhere to the D0-D4 classification definitions.
2. For all Applications designated as having D0 or D1 RTOs, Service Provider shall perform annual DR tests, except where directed otherwise by DIR and DIR Customers, and will complete the initial DR testing within twelve (12) months after the Commencement Date.
3. Upon DIR Customer request, Service Provider shall perform DR testing of any Application that has a D2 RTO, provided the DIR Customer requests the DR testing at least nine (9) months in advance of the proposed test date.
4. Upon DIR Customer request, Service Provider shall perform documented table top exercises for all Applications having D0, D1, D2 and D3 RTOs (not more frequently than annually), where no other DR testing has been performed.
5. In cooperation with DIR Customers, Service Provider shall conduct DR failover tests for Applications architected with high availability failover environments as requested by the DIR Customer; such failover tests may be conducted several times per year as required by Application criticality.
6. In conjunction with Application DR tests Service Provider shall include the associated Utility Servers and other related servers.

2.2.2 Disaster Recovery Testing for Email Services

1. Service Provider shall perform DR testing of email servers at least annually, and will complete the initial DR testing within twelve (12) months after the Commencement Date.
2. Service Provider shall in conjunction with Email DR tests, include the associated Infrastructure servers.

2.2.3 Disaster Recovery Testing for Consolidated Data Centers

1. Service Provider shall perform an annual enterprise DR table top exercise of each Consolidated Data Center, to include the Service Provider's Service Management Systems, in accordance with the applicable DRP.
2. The schedule for such testing shall be approved by DIR and appropriately coordinated with DIR and DIR Customers, providing the opportunity for DIR and DIR Customers to observe and participate in the test.

3. TRUE-UP OF INITIAL RTO LEVELS

1. For all Applications that have not been tested in the previous two (2) year period, within 120 days after the Commencement Date (to coincide with the Server Service Tier True-Up deadline), Service Provider shall provide a gap analysis between the requested RTO and the current Application's capability of achieving that RTO.
2. Service Provider shall update the DRP (including Technical Recovery Guide) and other infrastructure process such as backup schedules, if necessary, with changes needed to meet the RTO.
3. If the gap analysis determines technical changes are needed in order to meet the RTO, Service Provider will work with the DIR Customer to determine whether the RTO should be changed (downgraded to an achievable RTO based on the current technical environment) or whether the DIR customer needs to open a solution request for technical modifications.

4. SERVER SERVICE TIER RTO

Each Application that is addressed by a DRP has a designated RTO. DIR and DIR Customers will provide a priority for the recovery of Applications within the RTO. The RTO and priority information must be maintained in the CMDB.

Attachment 4-E describes the tiers of Servers, tiers of storage, and the Recovery Point Objectives (RPO).

1. The RTO for Applications are within one of the following categories:

DR Level	RTO	Viability of DRP
DP	1 hour	<ul style="list-style-type: none"> • DRP in place • DRP successfully tested
D0	24 hours	<ul style="list-style-type: none"> • DRP in place • DRP successfully tested
D1	72 hours	<ul style="list-style-type: none"> • DRP in place • DRP tested
D2	1 week	<ul style="list-style-type: none"> • DRP in place • DRP tested or table top exercised
D3	2 weeks +	<ul style="list-style-type: none"> • DRP in place • DRP table top exercised
D4	Low Priority, as part of Service Restore	<ul style="list-style-type: none"> • DRP in place

2. Service Provider shall perform DR Services to meet or exceed the applicable RTO for each Application, as indicated in the relevant DIR Customer DRP.
3. DIR Customers may change an Application’s DR Level rating, in accordance with the “DR Level Application Requirements” table below, upon 90-days notice to Service Provider. Service Provider will perform a technical assessment of the Application’s capability to meet the minimum requirements of the requested RTO, identifying any changes needed to meet the minimum requirements, and provide a schedule to the DIR Customer which implements those changes within the 90 days of the customer’s notice.

4.1 Disaster Recovery Level Application Requirements

1. To meet the RTOs, each Application will need to have appropriate supporting infrastructure, tools and management; as described in the following table:

DR Level	RTO	Minimum Requirements
DP	1 hour	<ul style="list-style-type: none"> • Application participates in annual test of DR capability with Service Provider and appropriate Third Parties • Application has alternate systems installed and managed in appropriate DR location • Application has appropriate data replication
D0	24 hours	<ul style="list-style-type: none"> • Application participates in annual test of DR capability with Service Provider and appropriate Third Parties • Application has alternate systems installed and managed in appropriate DR location • Application has appropriate data replication
D1	72 hours	<ul style="list-style-type: none"> • Application participates in annual test of DR capability with Service Provider and appropriate Third Parties • Application has alternate systems installed and managed in appropriate DR location • Application has appropriate data backup and restore methods and processes
D2	1 week	<ul style="list-style-type: none"> • Application participates in annual test or table top exercise of DR capability with Service Provider and appropriate Third Parties • Application has alternate systems installed in appropriate DR location • Application has appropriate data backup and restore methods and processes

DR Level	RTO	Minimum Requirements
D3	2 weeks +	<ul style="list-style-type: none"> • Application participates in annual table top test of DR capability with Service Provider and appropriate Third Parties • Application has alternate systems or support contracts available to deploy in an appropriate DR location • Application has appropriate data backup and restore methods and processes
D4	Low Priority, as part of Service Restore	<ul style="list-style-type: none"> • Application has appropriate data backup and restore methods and processes

2. Service Provider shall perform an initial true up of DR classifications with Application capabilities, as defined in this exhibit.
3. On an ongoing basis, Service Provider shall report to DIR and DIR Customer where Applications do not have appropriate methods to support an Application's DR Level rating, as part of Service Provider's quarterly DR Planning update and as part of Service Provider's quarterly Capacity Planning activities.
4. When an Application has not been included in DR Testing activities in more than two (2) years, Service Provider shall raise risks to DIR and DIR Customer, in conjunction with Risk Management, where Service Provider reasonably may not be able to meet that Application's RTO.
5. For all Applications, Service Provider shall review and validate the DIR Customer's RTO business need within the Transformation Services and provide an opportunity for the DIR Customer to request a change in the RTO. The Service Provider will ensure adequate capacity/Equipment upon completion of the Transformation Services in respect of such Application to be able to perform Application recovery at the DIR Customer's requested RTO DR Level.

5. DISASTER RECOVERY FOR UTILITY SERVERS

1. For those servers classified as Utility Servers, Service Provider will recover Utility Server functions within the RTO of the Applications they support. Examples of Utility Server functions are: Domain Name Service (DNS), Data Center LAN services, Network Security services, Network Appliances, Remote Access VPN services, and Utility Server Appliances.
2. Service Provider will work with DIR and each DIR Customer to confirm the mapping of Utility Servers to the complete support structure for Application Servers and update the CMDB with this information.
3. Depending upon how the affected Application Server maps back to a Utility Server (e.g. authentication server), Service Provider will provide the necessary recovery of the appropriate corresponding Utility Server functions to an alternate Consolidated Data Center or through a DR contract (e.g. BCRS, SunGard).

5.1 Utility Server Email / Directory Services

In addition to above general recovery requirements for Utility Servers, Service Provider shall restore the following functionality within the following timeframes:

	Consolidated Data Center Email	Legacy Data Center Email
Send/Receive capability - any type of email platform at a given point in time	24 Hours	1 week
Full email account information recovered	2 Weeks	2 Weeks

5.2 Utility Server File / Print

In addition to above general recovery requirements for Utility Servers, Service Provider shall restore the following functionality within the following timeframes:

	Consolidated Data Center File / Print	Legacy Data Center File / Print
File / Print Functionality	24 Hours	1 week
Full restore of File shares	1 Weeks	2 Weeks

6. OTHER CONSIDERATIONS

Related considerations for Service Provider support of DR.

- Business continuity planning for DIR Customer business shall remain a function retained by DIR Customers; the Service Provider supports the DIR Customer’s business continuity planning through appropriate IT Service continuity planning.
- DR and business continuity planning in respect of any sites, applications or systems that are managed, controlled or owned by the Service Provider shall be the responsibility of the Service Provider. This includes all tools, facilities and technologies the Service Provider uses to deliver the Services.
- DR planning in respect of out-of-scope equipment shall remain the responsibility of the DIR Customers.

6.1 Texas Emergency Management Council

Any disaster that potentially affects the Consolidated Data Centers and Non-Consolidated Service Locations will require DIR and the DCS Service Providers to interact with the State's Emergency Management Council ("the Council"). The Council, composed of thirty-two (32) agencies, the American Red Cross and The Salvation Army, is established by Law to advise and assist the Governor of the State in all matters relating to disaster mitigation, emergency preparedness, disaster response, and recovery.

During major emergencies, the Council representatives convene at the State Operations Center to provide advice on and assistance with response operations and coordinate the activation and deployment of State resources to respond to the emergency. Generally, State resources are deployed to assist local governments that have requested assistance because their own resources are inadequate to deal with an emergency. The Council is organized by emergency support function, or groupings of agencies, that have legal responsibility, expertise, or resources needed for a specific emergency response function.

7. ADDITIONAL REFERENCES

The Service Provider should reference the policies and guidelines of the following additional sections when providing the IT service continuity and DR requirements of this Exhibit:

- **Attachment 4-E** (Server Service Tier Matrix)
- **Exhibit 17** (Security and Safety)
- **Section A.4.5** (Crisis Management) of **Exhibit 2.1** (Multisourcing Service Integrator Statement of Work)
- **Section A.4.5** (Crisis Management) of **Exhibit 2.1.2** (Cross-Functional Services Statement of Work)

The Service Provider shall observe and obey all applicable Federal and State Laws (e.g. 1 TAC Chapter 202).