

**Appendix 5 to
Eleventh Amendment of
Master Services Agreement**

August 22, 2016



**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**

August 22, 2016

TABLE OF CONTENTS

1. INTRODUCTION..... 5

 2.1 Disaster Recovery Plan (DRP)..... 5

 2.2 Disaster Recovery Testing 6

 2.2.1 Disaster Recovery Testing for Server and Mainframe Services 7

 2.2.2 Disaster Recovery Testing for Email Services..... 7

 2.2.3 Disaster Recovery Testing for Consolidated Data Centers..... 7

 2.2.4 Disaster Recovery Testing for Active Directory Federation Services (ADFS) with Office 365 .7

3. TRUE-UP OF INITIAL RTO LEVELS 9

4. RECOVERY TIME OBJECTIVE (RTO)..... 10

 4.1 Disaster Recovery Level Application Requirements 12

 4.2 Server Service Tier 14

5. DISASTER RECOVERY FOR UTILITY SERVERS 15

 5.1 Utility Server Email / Directory Services /ADFS 15

 5.2 File / Print, Enterprise File, Remote File 15

6. OTHER CONSIDERATIONS..... 16

 6.1 Texas Emergency Management Council 17

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 support testing of all Third Party Disaster Recovery contracts in existence, and continue to support such contracts until such time that a successful test has been achieved for alternative solutions, or the DCS Customer requests the cancellation of the contract.
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 Class 1 RTO, and all necessary network, coupling facilities and channel resources required to meet the RTO.
5. If a disaster affects more than one data center, such as an LDC, and capacity is available to recover more than one affected site, the Service Provider shall proceed with recovery activities in accordance with Exhibit 16 consistent with the Statewide Functional Categories and RTOs.

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 annually 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 and Technical Recovery Guides 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 in accordance with applicable Laws and this Exhibit 16.

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 DIR Customer 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 impacts to active production, test, and development environments are minimized. If an active environment is required to execute the test, the use of the environment must be communicated and approved by the DIR Customer prior to the test.
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 DR classification definitions.
2. For all Applications designated as having Class P, Class 1 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 documented table top exercises, for all Applications eligible for testing, as described in the Service Management Manual (SMM), where no other DCS DR testing has been performed.
4. 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.
5. 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.
2. Service Service Provider shall in conjunction with Email DR tests, include the associated Infrastructure servers.
3. DR Testing for Email Services is available for DCS Customers that have not migrated to O365. For DCS Customers using O365, Service Provider will provide DR testing for O365 Federation Services as specified in Section 2.2.4.

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.

2.2.4 Disaster Recovery Testing for Active Directory Federation Services (ADFS) with Office 365

1. DIR Customers can request annual DR testing of ADFS services designated as having Class 1 RTOs. The DCS Customer is responsible for performing the O365 configurations to enable testing.
2. DR testing performed on ADFS servers will result in Agency production email services being unavailable while alternate ADFS services are brought on line to test and again when the service is returned to the primary servers.

3. ADFS servers with apps at Class 3 will be covered in the annual enterprise Class 3 tabletop exercise.
4. ITL testing for O365 Federation Services is not available.

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. RECOVERY TIME OBJECTIVE (RTO)

Each Application that is addressed by a DR Plan has a designated RTO. DIR and DIR Customers will designate a DR Class and a DR Functional Category Code that is used to establish a priority for the recovery of Applications within the RTO. The RTO and Category Code must be maintained in the CMDB.

1.1 The DR Functional Category Codes are described below:

Code	Summary	Description
SAFE	Physical Security and Safety and Public Health	Includes all systems that support functions protecting physical security and safety of individuals and the public including but not limited to law enforcement, criminal justice, protective and related services, and homeland security; and systems that protect against imminent threats to public health including but not limited to disease outbreak and sanitation.
ASST	Essential assistance to vulnerable populations	Includes all systems that provide financial, medical, or other life-sustaining (e.g., food, shelter) assistance benefits or services to eligible citizens such as aged, persons with disabilities, unemployed persons, and child support recipients. Includes both disaster-related support and continuation of ongoing benefits. The focus for this category is support for the individual beneficiary.
TRAN	Public transportation and movement of goods	Includes all systems that enable the use of roads, bridges, ports, airports, and other critical infrastructures and other ancillary support of transportation.
GOVT	Essential government administration	Includes all systems that enable essential government functions including but not limited to critical vendor payments and financial transactions, especially those activities which if not performed would result in a significant financial loss to the state. The focus of this item is the business of government and may include items that support the functions above.
REGU	Education, regulation, taxation, business and economic development and general government administration	Includes all systems supporting government functions not listed above, including but not limited to providing for education, regulating industry and business entities, collecting taxes, supporting business and economic development and general government.

2.1 Service Provider shall perform DR Services to meet or exceed the applicable RTO for each Application, as indicated in the relevant DIR Customer DRP and tracked in the CMDB.

3.1 DIR Customers may change an Application's DR Class Level, using the appropriate DCS process. 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 propose a solution, as needed, which implements those changes.

4.1 Disaster Recovery Level Application Requirements

- To meet the RTOs, each Application will need to have appropriate supporting infrastructure, tools and management; as described in the following table. Eligibility for DR testing for each DR Class also is noted.

DR Level	RTO	Minimum Requirements	DR Exercise Eligibility
Class P	1 hour	<ul style="list-style-type: none"> Application resides on servers within the Consolidated Data Centers Application has automatic failover Application has appropriate data replication 	<ul style="list-style-type: none"> Annual exercise of DR capability with Service Provider and appropriate Third Parties
Class 1	72 hours	<ul style="list-style-type: none"> Application resides on servers within the Consolidated Data Centers Application has identified target systems installed and managed in appropriate DR location Application has appropriate data replication 	<ul style="list-style-type: none"> Annual exercise of DR capability with Service Provider and appropriate Third Parties
Class 2A	7 days	<ul style="list-style-type: none"> Application resides on servers within the Consolidated Data Centers Application has identified target systems installed and managed in appropriate DR location with sufficient allocated storage. Application has appropriate data backup and restore methods and processes 	<ul style="list-style-type: none"> Annual exercise or table-top exercise of DR capability with Service Provider and appropriate Third Parties
Class 2B	14 days	<ul style="list-style-type: none"> Application has identified target systems installed in appropriate DR location with sufficient allocated storage. Application has appropriate data backup and restore methods and processes Application has compatible tape technologies at appropriate DR location. 	<ul style="list-style-type: none"> Annual exercise or table top exercise of DR capability with Service Provider and appropriate Third Parties

DR Level	RTO	Minimum Requirements	DR Exercise Eligibility
Class 3	21 days	<ul style="list-style-type: none"> • Application recovery is supported by “acquired at time of disaster” contracts from the Service Provider available to deploy in an appropriate DR location • Application has appropriate data backup and restore methods and processes • Application has compatible tape technologies at appropriate DR location. 	<ul style="list-style-type: none"> • Annual enterprise table-top exercise of DR capability with Service Provider and appropriate Third Parties • Application recovery is out of scope. • Upon request during annual planning cycle, annual DCS Customer table-top exercise of DR capability with Service Provider and appropriate Third Parties
Class 4	Low Priority, as part of Service Restore	<ul style="list-style-type: none"> • Application has appropriate data backup and restore methods and processes 	<ul style="list-style-type: none"> • No Exercise
Class 5	7 days	<ul style="list-style-type: none"> • Application resides on servers within the Consolidated Data Centers • Application has identified target systems installed and managed in appropriate DR location • Application has appropriate data replication • Application has non-transactional data only. 	<ul style="list-style-type: none"> • Annual exercise or table-top exercise of DR capability with Service Provider and appropriate Third Parties
Class 6	14 days	<ul style="list-style-type: none"> • Application resides on servers within the Consolidated Data Centers • Application has identified target systems installed and managed in appropriate DR location with sufficient allocated storage. • Application has non-Transactional Data only. Agency Assumes the risk that the application will provide acceptable performance on slower disk. • Application has appropriate data backup and restore methods and processes 	<ul style="list-style-type: none"> • Annual exercise or table top exercise of DR capability with Service Provider and appropriate Third Parties

DR Level	RTO	Minimum Requirements	DR Exercise Eligibility
Class 7	14 days	<ul style="list-style-type: none"> Application resides on servers within the Consolidated Data Centers Application has identified target systems installed and managed in appropriate DR location with sufficient allocated storage. Application has appropriate data backup and restore methods and processes Application has non-transactional data only. 	<ul style="list-style-type: none"> Annual exercise or table top exercise of DR capability with Service Provider and appropriate Third Parties
Class 8	As per the DR Recovery contract	<ul style="list-style-type: none"> Application has appropriate data backup and restore methods and processes 	<ul style="list-style-type: none"> Annual exercise of DR capability, as per DR contract, with Service Provider and appropriate Third Parties

- 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 annual DR Planning update and as part of Service Provider's annual Capacity Planning activities.
- 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.
- 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.

4.2 Server Service Tier

Attachment 4-E describes the tiers of Servers, tiers of storage, and the Recovery Point Objectives (RPO). The service tier does not determine the DR class; however, some DR classes may require a particular service tier.

5. DISASTER RECOVERY FOR UTILITY SERVERS

1. For those servers classified as Utility Servers, Service Provider will recover Utility Server functions as noted in the table below.
2. Service Provider will provide the necessary recovery of the appropriate corresponding Utility Server functions to an alternate **recovery site, such as a Consolidated Data Center**, or through a DR contract (e.g. BCRS, SunGard).

5.1 Utility Server Email / Directory Services / ADFS

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

	ADFS Server	Other Email Services
Send/Receive capability - any type of email platform at a given point in time	As per Server DR Capability	1 week
Full email account information recovered	N/A	2 Weeks

5.2 File / Print, Enterprise File, Remote File

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	As per Server DR Capability	As per Server DR Capability
Full restore of File shares	As per Server DR Capability	As per Server DR Capability
Enterprise File Services	As per Server DR Capability	N/A
Remote File Services	N/A	Class 3

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.
- DCS Customer Test Slots:
 - MSI will develop an Annual DR Test Plan and Schedule that will be limited to one full DR exercise test slot and one tabletop DR exercise test slot per DCS Customer.
 - After annual planning, the testing schedule and test slots can only be changed throughout the year by mutual agreement between DIR, SCP, and MSI.
 - MSI will provide an annual DCS Customer DR plan update for each DCS Customer.
 - A test slot lasts up to 1 week (7 calendar days).
 - Full DR exercises will be conducted for Class P, Class 1, and Class 8 applications.
 - All of the DCS Customer Class P, Class 1, and Class 8 applications are eligible to be tested in the full DR exercise test slot.
 - If the Integrated Test Lab (ITL) does not have sufficient capacity to support the Class 1 applications within the full DR exercise test slot, then additional test slots will be made available to the DCS Customer (only Class 1 applications require ITL resources).
 - DCS Customers are expected to maximize the ITL capacity in order to limit the number of test slots.
- Refer to **Exhibit 4** and **Attachment 4-E** in both MSI DIR-DCS-MSI-001 and SCP DIR-DCS-SCP-002 contracts for DR RU explanations.

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.