Appendix 5 to the
Second Amendment of
Master Services Agreement

DIR-MAS-SCP-RCR-001

April 10, 2018

Exhibit to Managed Application Services Service Component Provider Master Services Agreement

DIR Contract No. DIR-MAS-SCP-RCR-001

Between

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

and

Allied Consultants, Inc.

Exhibit 16

IT Service Continuity Management

Contract Change Log

Amendment/CCR #	Date	Description of Changes
Second Amendment/ CCR ####	January 30, 2018	• Removal of Class 5 and 7 from Disaster Recovery table. • Addition of Recovery Point Objective (RPO) and Class M to Disaster Recovery table. • Add language regarding reporting requirements that align with other Service Providers' Exhibit 16 Disaster Recovery requirements.

TABLE OF CONTENTS

1.0 INTRODUCTION

Disaster Recovery expectations are set forth in **Exhibit 2.7.1**, and **Exhibit 2.7.2.** Recovery of applications in the event of a disaster will require coordination between the MAS Service Providers and the DCS Service Providers.

For applications hosted in the DCS program, the DCS Service Providers are responsible for disaster recovery of the infrastructure and the MAS Service Providers are responsible for recovery of the application.

For development environments hosted outside DCS, the MAS Service Provider is responsible for disaster recovery of both the infrastructure and the application.

Rate Card Resources are required to follow the STC Customer's requirements and directions in the event of a disaster.

The Service Provider will prepare a Declaration Fee statement as part of the Service Proposal for the STC Customer's review and approval per **Exhibit 4**. The Declaration Fee must include costs to recovery the application at time of disaster as well as the costs to return that application and all other services to normal operations.

2.0 GENERAL DISASTER RECOVERY

2.1 Application Development

Service Provider is required to create and maintain disaster recovery plans and application recovery guidelines for applications in the development phase. If the development application is not hosted in DCS, Service Provider is required to maintain plans to recover both the infrastructure and the application, in accordance with **Section 3.5 of Exhibits 2.7.1 and 2.7.2.**

Service Provider is required to create disaster recovery plans and application recovery guidelines for production environments. These plans should assume the DCS Service Providers are responsible for infrastructure recovery.

Service Provider must establish declaration procedures, approved by DIR, and document those procedures in the Service Management Manual.

Service Provider will schedule, plan and perform Disaster Recovery Testing for application development or test environments hosted outside DCS, if required by the STC Customer.

Service Provider will be responsible for providing the resources needed to support the disaster recovery strategy.

In the event of a disaster, the DCS Service Providers are responsible for initiating recovery activities. Service Provider is required to coordinate application recovery activities with the DCS Service Providers. If the development application is not hosted within DCS, Service Provider is required to execute the disaster recovery plan and recover both the infrastructure and application within the STC Customer's required timeframes.

In the event of a disaster, Service Provider will continue to be liable for preparing and submitting deliverables, unless the STC Customer submits a waiver in writing.

2.2 Application Maintenance

Service Providers are required to maintain disaster recovery plans and application recovery guidelines for all application environments, as required by the STC Customer. These plans should assume the DCS Service Providers are responsible for infrastructure recovery. If a customer does not have a disaster recovery plan or application recovery guidelines at commencement of services, the Service Provider must coordinate with the MSI to create the plan and guidelines within three months of commencement.

Service Providers must establish declaration procedures, approved by DIR, and document those procedures in the Service Management Manual.

Service Provider will work with the DCS Service Providers to schedule, plan and perform Disaster Recovery Testing as required by the customer for production applications. Service Provider will coordinate with the DCS Service Provider's and the MSI's annual testing schedule to ensure recoverability of application and infrastructure.

Service Provider will be responsible for providing the resources needed to support the disaster recovery strategy.

In the event of a disaster, Service Provider be responsible for recovering the application within the Customer's required timeframe and to resume maintenance services. The DCS Service Providers are responsible for executing disaster recovery plans for the infrastructure, and MAS Service Providers are required to assist with the infrastructure recovery, execute application recovery guidelines and test applications. Service Provider must use commercially reasonable efforts to meet all maintenance service levels and deliverables.

2.3 Rate Card Resources

STC Customers may request rate card resources to assist in the event of a disaster. Service Provider will be responsible for providing staff capable of assisting in application recovery.

2.4 RESERVED

3.0 RECOVERY TIME OBJECTIVE (RTO)

Each Application that is addressed by a Disaster Recovery Plan (DRP) has a designated Return To Operations (RTO). The Application may additionally have a Return to Normal (RTN) designation. DIR and STC 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 code must be maintained in the MSI's Configuration Management Data Base (CMDB).

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, which must be restored within the designated disaster recovery window.

1. Service Provider shall perform Disaster Recovery Services to meet or exceed the applicable RTO for each Application, as indicated in the relevant Customer Disaster Recovery Plan and tracked in the CMDB.

2. STC Customers may change an Application's DR Class, using the appropriate Service Management Manual 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.

3.1 Disaster Recovery Class -Application Requirements

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	RPO	Minimum Requirements
Class P	**1 hour**	• **1 hour**	• Application resides on servers within the Consolidated Data Centers • Application participates in annual exercise of DR capability with Service Provider and appropriate Third Parties • Application has automatic failover • Application has appropriate data replication
Class M	**24 hours**	• **1 hour**	• Application resides on Mainframes within the Consolidated Data Centers • Application has identified target Mainframes installed and managed in appropriate DR location • Application has appropriate data replication
Class 1	**72 hours**	• **6 hours**	• Application resides on servers within the Consolidated Data Centers • Application participates in annual test of DR capability with Service Provider and appropriate Third Parties • Application has identified target systems installed and managed in appropriate DR location. Application has appropriate data replication
Class 2A	**7 days**	• **48 hours**	• Application resides on servers within the Consolidated Data Centers • Application participates in scheduled test or table-top exercise of DR capability with Service Provider and appropriate Third Parties • 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
Class 2B	**14 days**	• **48 hours**	• Application participates in scheduled annual test or table top exercise of DR capability with Service Provider and appropriate Third • 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.

DR Level	RTO	RPO	Minimum Requirements
Class 3	**21 days**	• **48 hours**	• Application participates in annual table top test of DR capability with Service Provider and appropriate Third Parties • Application recovery is supported by "acquired at time of disaster" contracts from the Service Provider available to deploy in an appropriate DR location • Application must reside on supported Operating System, Middleware & Database versions, because physical instances will be recovered as virtual instances • Application has appropriate data backup and restore methods and processes • Application has compatible tape technologies at appropriate DR location.
Class 4	**Low Priority, as part of Service Restore**	• **Low Priority, as part of Service Restore**	• Application has appropriate data backup and restore methods and processes
Class 6	**14 days**	• **48 hours**	• 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. • 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

DR Level	RTO	RPO	Minimum Requirements
Class 8	**As per the DR Recovery contract**	• **As per the DR Recovery contract**	• Application participates in scheduled test of DR capability with Service Provider and appropriate Third Parties • Application has appropriate data backup and restore methods and processes

1. 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.

2. 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.

3. 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.

4.0 OTHER CONSIDERATIONS

Related considerations for Service Provider support of DR.

a. Business continuity planning for STC Customer business shall remain a function retained by STC Customers; the Service Provider supports the STC Customer's business continuity planning through appropriate IT Service continuity planning.

b. 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.

5.0 ADDITIONAL REFERENCES

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

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