

**MASTER SERVICES AGREEMENT**

between

**THE STATE OF TEXAS, ACTING BY AND THROUGH  
THE TEXAS DEPARTMENT OF INFORMATION RESOURCES**

and

**INTERNATIONAL BUSINESS MACHINES CORPORATION**

**DATED NOVEMBER 22, 2006**

**EXHIBIT 16**

**IT DISASTER RECOVERY PLAN**

**EXHIBIT 16**

**IT DISASTER RECOVERY PLAN**

**TABLE OF CONTENTS**

**1.0 INTRODUCTION..... 1**

**2.0 DR SERVICES FOR APPLICATIONS WITH EXISTING DR PLANS..... 2**

**3.0 DR SERVICES FOR APPLICATIONS WITHOUT EXISTING DR PLANS ..... 3**

**4.0 DR SERVICES AT COMPLETION OF TRANSFORMATION ..... 4**

**5.0 DISASTER RECOVERY FOR UTILITY SERVERS ..... 5**

**6.0 OTHER CONSIDERATIONS..... 5**

**7.0 STANDARD DISASTER RECOVERY PLAN CONTENTS..... 6**

    7.1 Background..... 6

    7.2 Scope..... 6

    7.3 IT Disaster Declaration Criteria..... 6

    7.4 IT Call Out Procedure ..... 7

    7.5 Contingency Mode Resource Plan ..... 7

    7.6 Key Documents and Procedures ..... 7

    7.7 Notification and Reporting..... 7

    7.8 Mainframe Recovery Activities and Procedures..... 8

    7.9 Servers Recovery Activities and Procedures ..... 8

    7.10 Network Recovery Activities and Procedures ..... 8

    7.11 Other Cross Functional Recovery Activities and Procedures ..... 8

    7.12 Return to Normal Operating Mode ..... 8

    7.13 Training and Test Procedures ..... 8

## **1.0 INTRODUCTION**

Upon the occurrence of a disaster under the applicable disaster recovery plan, 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 disaster recovery plans.

## 2.0 DR SERVICES FOR APPLICATIONS WITH EXISTING DR PLANS

For those DIR Customers receiving the Services upon the Commencement Date that have documented disaster recovery plans as of such date, Service Provider shall perform Disaster Recovery Services in accordance with the requirements of this Section:

1. Service Provider shall provide DR Services in accordance with each such disaster recovery plan.
2. Each Application that is addressed by such disaster recovery plans has a designated recovery time objective (“**RTO**”) that falls within one of the following categories:

Disaster Recovery Priority	Recovery Time Objective (RTO)	Viability of Plan
D0	24 hrs	<ul style="list-style-type: none"> <li>• DRP in place</li> <li>• DRP successfully tested</li> </ul>
D1	72 hrs	<ul style="list-style-type: none"> <li>• DRP in place</li> <li>• DRP tested</li> </ul>
D2	1 week	<ul style="list-style-type: none"> <li>• DRP in place</li> <li>• Equipment provided for</li> <li>• DRP desktop exercised</li> </ul>
D3	2 weeks +	<ul style="list-style-type: none"> <li>• DRP in place</li> <li>• DRP desktop exercised</li> </ul>
D4	Low Priority, Agency Discretion, as resources are available	<ul style="list-style-type: none"> <li>• DRP in place</li> </ul>

3. Service Provider shall perform DR Services so as to meet or exceed the applicable RTO for each Application, as indicated in the relevant DIR Customer disaster recovery plan.
4. For all Applications designated as having a D0, D1, D2, D3 or D4 RTO, within three (3) months after the Commencement Date, Service Provider shall update all existing DIR Customer-specific disaster recovery plans to reflect all changes implemented during the performance of Transition Services.
5. For all Applications designated as having D0 or D1 RTO’s, Service Provider will complete disaster recovery testing within twelve (12) months after the

Commencement Date and annually thereafter. Each such test shall address the specific needs of each DIR Customer for coordination with Service Provider and at a minimum shall demonstrate Service Provider’s ability to meet or exceed the designated RTO’s for those Applications in the event of a disaster.

**3.0 DR SERVICES FOR APPLICATIONS WITHOUT EXISTING DR PLANS**

For those DIR Customers receiving the Services upon the Commencement Date that do not have documented disaster recovery plans as of such date, Service Provider shall perform Disaster Recovery Services in accordance with the requirements of this Section:

1. Applications that are not addressed by a disaster recovery plan but are designated by a DIR Customer as important to its operations shall have one of the following RTO’s, as designated by the applicable DIR Customer:

<b>Disaster Recovery Priority</b>	<b>Recovery Time Objective</b>
T1*	72 hrs
T2	1 week
T3	2 weeks +
T4	Low priority, DIR Customer discretion, as resources are available

\* T1 designation reserved for mission critical Applications.

2. Service Provider shall perform DR Services so as to meet or exceed the applicable RTO set forth in this Section as designated by the applicable DIR Customer for each Application until the completion of Transformation Services in respect of such Application. Thereafter, the applicable DIR Customer shall designate such Application as having one of the RTO’s set forth in Section 2, and Service Provider shall perform DR Services so as to meet or exceed the RTO designated in respect of such Application.
3. For all Applications designated as having a T1, T2, T3 or T4 RTO, within three (3) months after the Commencement Date, Service Provider shall provide a draft of an interim disaster recovery plan for the applicable DIR Customer’s review and approval that documents and demonstrates Service Provider’s plan and capability to restore those Applications within their applicable RTO’s.
4. For all Applications designated as having a T1 or T2 RTO’s, within nine (9) months after the Commencement Date, Service Provider shall provide a final disaster recovery plan for the applicable DIR Customer’s review and approval that clearly documents and demonstrates Service Provider’s plan and capability to restore those Applications within their applicable RTO’s.

5. For each Application designated as having a T1 RTO, Service Provider shall provide adequate capacity/Equipment upon completion of the Transformation Services in respect of such Application to be able to perform Application recovery as a D1 Disaster Recovery Priority. Service Provider must complete Disaster Recovery testing for Applications having T1 RTO's prior to the completion of Transformation Services within twelve (12) months after the completion of Transformation Services in respect of each such Application. Each such test shall address the specific needs of each applicable DIR Customer for coordination with Service Provider and at a minimum shall demonstrate Service Provider's ability to meet or exceed the designated RTO's for those Applications in the event of a disaster.

#### **4.0 DR SERVICES AT COMPLETION OF TRANSFORMATION**

For all DIR Customers receiving the Services upon the Commencement Date, Service Provider shall provide the following Disaster Recovery Services:

1. Service Provider shall develop, maintain and implement a comprehensive disaster recovery plan for the DIR Customers and DIR Customer-specific disaster recovery plans, in each case subject to DIR's prior review and approval.
2. Within three (3) months after the completion of Transformation Services in respect of the first DIR Customer for which Transformation Services are performed, Service Provider shall develop and provide for DIR's review and approval a consolidated disaster recovery plan for the DIR Consolidated Data Centers and Service Provider Consolidated Data Centers which shall document the processes and procedures that will be used for testing, disaster declaration, interim operations in the event of a disaster and recovery of facilities and Equipment necessary to restore the DIR Consolidated Data Centers to their original operational capacity. Such plan shall be updated at least once each quarter to reflect all changes implemented over the course of Service Provider's performance of the Transformation Services.
3. Service Provider will adjust the applicable disaster recovery plans whenever a DIR Customer's needs change.
4. Service Provider shall perform disaster recovery testing for simultaneous recovery of all Applications that have a D1 RTO and are located at each DIR Consolidated Data Center at least annually. Service Provider shall perform disaster recovery testing of all Applications that have a D2 RTO as required by the applicable DIR Customer(s) which are scheduled at least nine (9) months in advance of the proposed test date. Service Provider shall perform documented desktop exercises for all Applications having D2 and D3 RTO's at least annually.
5. All disaster recovery plans 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 annually in accordance with applicable Laws.

**5.0 DISASTER RECOVERY FOR UTILITY SERVERS**

Once the classification has been verified for each of the Application Servers, Service Provider will work with DIR and each DIR Customer to confirm the mapping of the complete support structure for the Application Servers. Depending upon how the affected Application Server maps back to a Utility Server (e.g., authentication server), Service Provider will provide the necessary recovery for the appropriate corresponding Utility Server functions within the corresponding Data Center or through a BCRS/SunGard type solution.

Notwithstanding the generality of the foregoing, Service Provider shall restore the following System-level functionality for up to 30,000 e-mail accounts within the following timeframes:

	Prior to completion of Transformation Services	Following completion of Transformation Services
Send/Receive capability - any type of email platform at a given point in time	72 Hours	48 Hours
Full e-mail account information recovered	14 Days	14 Days

Service Provider expects to restore such functionality using Service Provider’s Dallas Data Center. DIR will be responsible for providing WAN/Internet connectivity to/from such facility and for any necessary Application-related support.

Recovery will be implemented using a shared framework consisting of standard policies across all users. Any special security or technical restrictions for specific groups of users will be limited.

Until implementation of the enterprise-wide disaster recovery solution as part of the Transformation Services, Service Provider will provide the e-mail-related restoration capability provided under disaster recovery agreements between DIR Customers and Third Party Vendors that are in effect as of the Effective Date.

**6.0 OTHER CONSIDERATIONS**

- Business continuity planning shall remain a function retained by DIR
- Disaster recovery planning in respect of any sites that are managed, controlled or owned by Service Provider shall be the responsibility of Service Provider

- Disaster recovery planning in respect of out-of-scope equipment shall remain the responsibility of the DIR Customers. The necessary services may be requested through the Service Provider.
- In addition to disaster recovery tests conducted individually for each DIR Customer, Service Provider shall conduct at least annually a consolidated disaster recovery test of each DIR Consolidated Data Center and DIR Service Provider Consolidated Data Center for Disaster Recovery Priority D1 Applications, and shall test all other Applications in accordance with the applicable disaster recovery plan.
- Any disaster that affects the Data Centers will require DIR and Service Provider to interact with the State's Emergency Management Council ("EMC"). The EMC, composed of thirty (30) 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, EMC 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 EMC is organized by emergency support function, or groupings of agencies that have legal responsibility, expertise, or resources needed for a specific emergency response function.

## **7.0 STANDARD DISASTER RECOVERY PLAN CONTENTS**

All disaster recovery plans that are developed by Service Provider shall address the following topics, in whole or in part, unless otherwise directed by DIR:

### **7.1 Background**

#### **7.1.1 Purpose**

#### **7.1.2 Goals and Objectives**

#### **7.1.3 Benefits**

### **7.2 Scope**

#### **7.2.1 Policies**

#### **7.2.2 Overview**

### **7.3 IT Disaster Declaration Criteria**

#### **7.3.1 Operational Priorities**

**7.3.2 Levels of Response**

**7.3.3 Procedures for Invoking Contingency Mode**

**7.3.4 Required Authorizations**

**7.3.5 Notification Procedures**

**7.3.6 Media Handling Procedures**

**7.4 IT Call Out Procedure**

**7.5 Contingency Mode Resource Plan**

**7.5.1 Functional Org Chart**

**7.5.2 Teams Roles and Responsibilities**

**7.5.3 Recovery Team Director**

**7.5.4 Command Center Coordinator**

**7.5.5 Recovery Team Leaders**

**7.5.6 Recovery Teams**

**7.5.7 Key Personnel Emergency Contact List**

**7.5.8 Key Service Providers and Vendors Contact List**

**7.5.9 Manpower Recovery Strategy**

**7.6 Key Documents and Procedures**

**7.6.1 Documents and Records Vital to IT Processes**

**7.6.2 Emergency Stationery and Office Supplies**

**7.6.3 Emergency Office Equipment**

**7.7 Notification and Reporting**

**7.7.1 Notifying and Mobilizing the Teams**

**7.7.2 Notifying Management and Key Employees**

**7.7.3 Handling Personnel Family Notification**

**7.7.4 Handling Media**

**7.7.5 Maintaining Event Log**

**7.7.6 Phase Reporting**

**7.8 Mainframe Recovery Activities and Procedures**

**7.9 Servers Recovery Activities and Procedures**

**7.10 Network Recovery Activities and Procedures**

**7.11 Other Cross Functional Recovery Activities and Procedures**

**7.12 Return to Normal Operating Mode**

**7.12.1 Criteria for Returning to Normal Operating Mode**

**7.12.2 Procedures for Returning to Normal Operating Mode**

**7.12.3 Procedures for Recovering Lost or Damaged Information**

**7.12.4 Detailed Lists, Inventories and Services Required**

**7.13 Training and Test Procedures**

**7.13.1 Managing the Training Process**

**7.13.2 Training Process and Schedule**

**7.13.2.1 Team Training**

**7.13.2.2 User Training**

**7.13.3 Risk Management**

**7.13.4 Testing of Recovery Plan**

**7.13.4.1 Planning the Tests**

**7.13.4.2 Scheduling the Tests**

**7.13.4.3 Conducting the Tests**

**7.13.4.4 Test Schedule**

**7.13.4.5 Test Scenario**

**7.13.4.6 Test Monitoring**