

**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 17**

**SAFETY AND SECURITY PROCEDURES**

**EXHIBIT 17****SAFETY AND SECURITY PROCEDURES****1.0 INTRODUCTION**

In performing the Services and using the DIR Facilities, Service Provider shall observe and comply with the policies, rules, procedures and regulations set forth or referenced in this Exhibit.

The following Attachments are hereby incorporated into and deemed part of this Exhibit, and all references in this Agreement to this Exhibit shall be read and understood to include the following Attachments:

1. **Attachment 17-A**, which contains the policies, rules, procedures and regulations associated with data security;
2. **Attachment 17-B**, which contains the policies, rules, procedures and regulations associated with physical security at the Data Centers; and
3. **Attachment 17-C**, which contains the procedures associated with performing and completing the security assessments described in Section 3 to this Exhibit and **Attachment 17-C**.

Service Provider acknowledges that **Attachment 17-A** and **Attachment 17-B** shall be amended by DIR from time to time after the Effective Date. Following delivery by DIR, Service Provider shall observe and comply with the terms and conditions of the amended versions of **Attachment 17-A** and **Attachment 17-B** provided by DIR, and the amended versions of **Attachment 17-A** and **Attachment 17-B** provided by DIR shall replace in their entirety the then-current versions of **Attachment 17-A** and **Attachment 17-B** without the need for any further action by the Parties.

**2.0 SAFETY AND SECURITY**

Service Provider shall:

1. Adhere to the then-current safety and security policies, rules, procedures and regulations established by the State and DIR, and each DIR Customer with respect to such DIR Customer's data and facilities.
2. Adhere to DIR's then-current "Security Rules," as published in "Chapter 202, Information Security Standards" of the Texas Administrative Code.
3. Without limiting Service Provider's obligations under Section 2.3 of **Attachment 17-B**, conduct national fingerprint-based criminal history record checks of all Service Provider Personnel having access to data that is protected and controlled under the Federal Bureau of Investigation's ("FBI") Criminal Justice Information Systems ("CJIS") Security Policy within thirty (30) days of each such individual's initial employment or assignment to the DIR account, and coordinate the clearance of Service Provider Personnel with appropriate DIR Customers.
4. Comply in all respects with the then-current versions of the FBI's "CJIS Security Addendum" and the FBI's "CJIS Security Policy."

5. Adhere to the then-current “Department of Information Resources Policy/Procedures Manual,” Section 3 - Human Resources, Subject 026 - Criminal History Policy.

### **3.0 SECURITY PLAN ASSESSMENTS**

DIR may initiate and conduct assessments of Service Provider’s security plans under and in accordance with **Attachment 17-C**. Such assessments will evaluate Service Provider’s abilities and capabilities in maintaining and enhancing security and safety practices and procedures, and may involve monitoring and testing security programs, conducting risk assessments and performing security design reviews.