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 17

Safety and Security

January 30, 2017

TABLE OF CONTENTS

1. INTRODUCTION

In performing the Services, all Service Providers shall observe and comply with the policies, rules, procedures and regulations set forth or referenced in this Exhibit.

Application Maintenance Services are required to use DCS infrastructure. Therefore, Service Provider must ensure it meets the DCS physical and logical security requirements, in addition to ensuring the safety and security of the STC Customer's application and data.

Application Development Services are required to architect to DCS standards and deploy the production version of the application in the DCS program. However, for test and development environments, Service Provider may choose whether to use its own infrastructure or use DCS infrastructure. If the Service Provider chooses to use its own infrastructure, the Service Provider must adhere to the physical and logical security requirements contained in this exhibit and the Service Provider's security policy and procedures must meet the level of the DCS security policies and procedures contained the the DCS Services Management Manual.

Rate Card Resources staff must comply with the physical and logical security of the STC Customer.

2. SAFETY AND SECURITY

The Service Provider's responsibilities include and the Service Provider will do the following:

1. Adhere to the then-current safety and security policies, rules, procedures and regulations established by the State and DIR, and each STC Customer with respect to such STC Customer's data.

   1.1. For Application Development: Adhere to physical and logical security requirements for development environments if not hosted within the Data Center Services (DCS) program. If development environments are hosted within DCS, adhere to DCS safety and security policies and procedures established in the DCS Services Management Manual

   1.2. For Application Maintenance: Adhere to physical and logical security policies and procedures defined in the DCS Services Management Manual.

   1.3. For Rate Card Resources: Adhere to each STC Customer's physical and logical security requirements, and to the requirements defined in this **Exhibit 17**.

2. Adhere to DIR and STC Customer's then-current "Security Rules," as published in Chapter 202, Information Security Standards of the Texas Administrative Code.

3. The Service Providers shall comply with the policies defined by the FBI Criminal Justice Information Services (CJIS) requirements.

4. DIR and STC Customers comply with National Institute of Standards and Technology (NIST) Federal standards and related NIST 800 series Special Publications (SP) and Federal Information Processing Standards (FIPS) standards. Where there is a conflict between NIST, FIPS and 1 TAC Chapter 202 rules and security controls, the 1 TAC Chapter 202 takes precedence. Service Providers are required to adhere to these standards.

5. Comply with all security incident notification and response procedures as specified in the Service Management Manual.

3. SECURITY ASSESSMENTS

DIR, STC Customers, Texas State Auditor's Office, and other entities authorized by DIR may conduct security reviews, assessments, forensic analysis and/or audits (e.g.SSAE 16, State Audit Office, IRS audits) of the infrastructure where service is being provided by the Service Provider. These assessments may include (but are not limited to) physical security, logical security, policies and procedures, network analysis, vulnerability scans and Controlled Penetration Tests.

Rate Card Resources are not subject to these security assessments.

4. CRIMINAL HISTORY BACKGROUND CHECKS

The Application Development, Application Maintenance and Rate Card Resources Service Providers must comply with this requirement for criminal history background checks if the Customer requests CJIS compliant background checks. If the Customer does not require CJIS background checks, then Service Provider shall perform background checks compliant with its company policy.

1. The SMM will define Service Provider staff required to successfully complete a background and criminal history investigation prior to performing contract functions or accessing DIR/STC Customer facilities, systems, networks or data under this contract. Criminal history background checks are to be conducted per Texas Government Code (TGC) Subchapter F, Section 411.1404 and will be in compliance with the then-current versions of the FBI CJIS Security Policy and the FBI CJIS Security Addendum. In addition, an annual background check re-verification is required. DIR must be notified of the compliance with the initial criminal history background check and the annual re-verification. The Service Provider is responsible for any costs associated with this process.

2. Background and criminal history investigations will be performed by the Texas Department of Public Safety, Texas Department of Criminal Justice, and the Texas Department of Family and Protective Services. Other STC Customers may require additional levels of compliance as per agency regulations and policies.

3. The MSI has a comprehensive security clearance database capable of tracking and reporting on all STC Service Provider personnel. All persons having been cleared are reported to the MSI and documented in the Security Clearance Database. The Service Provider will establish a process and reporting procedure, approved by DIR, which will provide timely notifications and updates of the database of personnel who are added to or depart from the contract. Reports will be provided no later than 24 hours after employee departure from the contract. Documented policies for this requirement will be drafted by the MSI and approved by DIR.

5. FEDERAL AND STATE LAWS

The Service Provider shall perform the Services in compliance with all federal and state laws and industry standards as they may be updated from time-to-time, including but not limited to the following:

- Texas Administrative Code (TAC) 1 Chapter 202. TAC 202 provides the State of Texas security standards policies applicable to all Texas state agencies.
- HIPAA – Health Insurance Portability and Accountability Act Privacy and Security Rules
- HITECH – Health Information Technology for Economic and Clinical Health Act
- FIPS 140-2 Federal Information Processing Standards Publication, Security Requirements for Cryptographic Modules

- FISMA – Federal Information Security Management Act
- FERPA – Family Educational Rights and Privacy Act
- IRS Pub 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies
- PCI – Payment Card Industry Security Standards
- ISO/IEC 27001:2005 - Information technology – Security techniques – Information security management
- ISO/IEC 27002 – code of practice for information security management
- NIST 800 – National Institute of Standards and Technology standards and related publications
- CJIS Security Policy - FBI Criminal Justice Information System Security Policy and CJIS Security Addendum