Exhibit to Managed Security Services Service Component Provider Master Services Agreement

DIR Contract No. DIR-MSS-SCP-001

Between

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

and

AT&T Corp.

Exhibit 2.1.2

Cross Functional Services Statement of Work

October 26, 201

Table of Contents

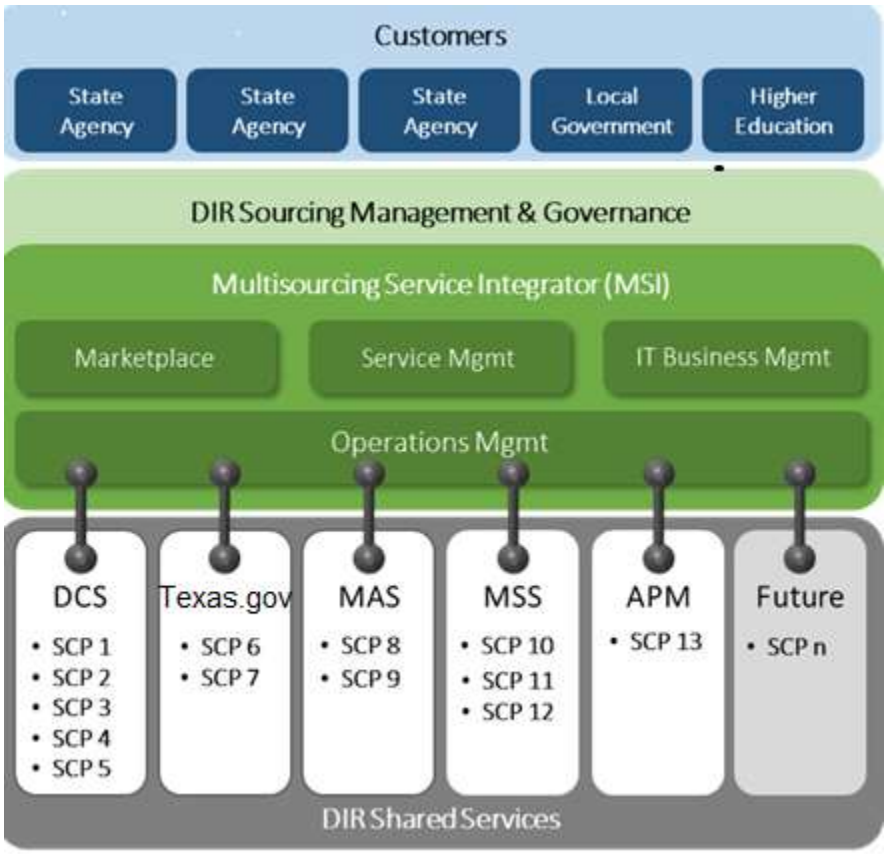
1 INTRODUCTION

1.1 Operating Model

This Exhibit contains specific functional requirements that all Service Component Providers (SCPs) (including the Service Provider) must meet in order to perform the requested Services and responsibilities defined in **Exhibits 2.8.1, 2.8.2, and 2.8.3**. Service Providers must integrate with DIR's Multi-sourcing Services Integrator (MSI).

DIR contracts with multiple SCPs to deliver shared technology services to DIR Customers. Those services are integrated into a common service delivery model by DIR's MSI. The MSI provides the systems, processes and service delivery oversight necessary to ensure consistent, quality service delivery. Figure 1 below depicts the relationships between SCPs and the MSI.

Figure 1



1.2 Document Overview

This document contains Service Management categories of responsibilities that apply to the delivery of Services. These categories are considered "cross-functional" in that they are functions which cross all SCPs.

1.3 Shared Services Systems and Processes

DIR bases its service management practices on the Information Technology Infrastructure Library (ITIL), which focuses on the service management lifecycle and the linkages between service management components. The Service Provider shall be responsible for using management practices complying with the ITIL framework in cooperation with and as established by the MSI.

1.3.1 Shared Services Processes

The Service Provider shall, at a minimum:

1.3.1.1 Conform and deliver to a set of processes based on ITIL guidance to enable consistent management of IT services seamlessly across the MSI and among SCPs.

1.3.1.2 Ensure that processes effectively integrate with the processes, functions and roles deployed within and used by DIR Customers, MSI, and the other SCPs.

1.3.1.3 Design processes and procedures to enable the effective monitoring and reporting of Service Provider's Services.

1.3.1.4 Coordinate the execution of Service Provider processes across DIR Customers and with the MSI to ensure all the individual components that make up the required Services are managed in an end-to-end manner.

1.3.1.5 Document Service Provider-level processes and procedures in the integrated Service Management Manual (SMM).

1.3.1.6 Deploy any necessary processes, procedures, and controls to provide effective end-to-end management, monitoring, and reporting of the Services.

1.3.1.7 Deploy and integrate any tools and systems necessary to enable such processes, procedures, and controls.

1.3.1.8 Implement change and configuration management for systems, services, and components managed by Service Provider.

1.3.1.9 Maintain security Tools to meet performance standards, processes and policies requirements, to maximize efficiency, and to minimize outages, as necessary.

1.3.1.10 Provide audit logs for any systems managed by the Service Provider.

1.3.2 Shared Services Documentation

All documentation maintained by the Service Provider shall be subject to approval by DIR and will conform to the documentation standards and format provided by the MSI and agreed upon between DIR and the Service Provider. The Service Provider shall develop documentation in accordance with the requirements in **Attachment 6-B Service Management Manual**.

The Service Provider shall, at a minimum:

1.3.2.1 Ensure that operations documentation related to the Services is up to date, accurate, and posted in the MSI's SMM.

1.3.2.1.1 Identify owners (business, operational, quality assurance, and engineering) of documentation.

1.3.2.1.2 Link Systems documentation to architectural standards.

1.3.2.1.3 Identify DIR Data to the associated System(s) and the associated security risk classification.

1.3.2.1.4 Provide access to architecture and design documentation for Systems and services managed by Service Provider.

1.3.2.1.5 Create and maintain current documentation as required (e.g., support documentation).

1.3.2.2 Develop and maintain documentation on all Operations procedures, Services, Equipment, and Software for which Service Provider is responsible.

1.3.2.3 Make all documentation available electronically.

1.3.2.4 Validate documentation annually for completeness and accuracy, and verify that all documentation is present, organized, readable, and updated in accordance with agreed upon schedule.

1.3.2.5 Participate in the reporting of validation findings to DIR and DIR Customers on a regular basis, and where it is determined that documentation is inaccurate (e.g., erroneous or out of date), correct and replace such documentation.

1.3.2.6 Update the SMM according to schedule described for the Critical Deliverables in **Exhibit 3-C Critical Deliverables**.

1.3.3 Training & Education

The Service Provider shall, at a minimum:

1.3.3.1 Support the MSI as appropriate to ensure the proper training on Service Management Systems and other tools, including the supporting processes, for Service Provider personnel.

1.3.3.2 Develop training content (as applicable to the awarded Service Component) and coordinate with the MSI to load and manage within the MSI-provided Learning Management System (LMS).

1.3.3.3 Customize such training to be specific to the Authorized Users for the Services within the DIR environment.

1.3.3.4 Schedule and provide training on the applicable Service Component for new Authorized Users based on the needs of DIR or DIR Customers. Create and maintain training material for Service Provider staff that includes at least the following information: The Services provided, the value of Services to DIR, the financial structure of charges, overview of DIR and DIR Customers, DIR Security Policies, orientation to all applicable laws and regulations (e.g., 1 TAC 202, HIPAA), the location of document stores, and the structure and location of the SMM.

1.3.3.5 Ensure that all staff interacting with DIR or DIR Customers have reviewed the minimum set of documentation.

1.3.3.6 Upon request, Service Provider shall provide such documentation and training to DIR and DIR Customers as specified by DIR.

2 MARKETPLACE

2.1 Portal

The Service Provider must leverage the MSI-provided Portal to provide integrated DIR and Customer communications and reporting. Reporting functions and specific operational reports are defined in **Exhibit 3 Service Levels**, and **Exhibit 13 Reports**.
The Service Provider shall, at a minimum:

2.1.1.1 Provide the MSI with the reports and communication content to be posted.

2.1.1.2 Provide reports and communication content in the format and standards required of the MSI's online portal.

2.1.1.3 Adhere to established processes as documented in the SMM.

2.2 Service Catalog Management

The MSI provides the Service Catalog tool for DIR Customers to request Services from the Service Provider.
The Service Provider shall, at a minimum:

2.2.1.1 Coordinate with the MSI to ensure integration of Service Provider Services into the Service Catalog.

2.2.1.2 Support the MSI to categorize and normalize Service Catalog content.

2.2.1.3 Support the MSI to determine the approval authority required to obtain the Service.

2.2.1.4 Support the MSI to document Service descriptions and dependencies.

2.2.1.5 Participate, through the MSI, in regular communications with DIR and DIR Customers on updates to the Service Catalog.

2.2.1.6 Respond to Service Catalog requests in accordance with defined processes and Service Level Agreements (SLAs).

2.3 IT Service Desk

Service Provider shall be responsible for responding to incidents or requests DIR Customers log with the MSI's Service Desk, in compliance with policies and procedures set forth in the SMM and managed by the MSI.

The MSI's Service Desk shall be the single point of contact for Authorized Users regarding Incidents, which include events that cause or may cause an interruption or reduction of service, as well as for requests for information and requests for services relating to all of DIR's and DIR Customers' IT Services.

The Service Provider shall, at a minimum:

2.3.1.1 Actively participate with the MSI to develop and document processes.

2.3.1.2 Integrate Service Provider's Service processes with the Service Desk processes of the MSI, DIR Customer, and authorized Third Party Vendor(s), where the processes interact.

2.3.1.3 Actively support the MSI to assure the proper application of Service Desk across all functions and organizations that provide services to DIR Customers.

2.3.1.4 Communicate and coordinate the Service Desk processes and policies within Service Provider's own organization and DIR Customers.

2.3.1.5 Actively participate in defining Service Desk policies and procedures, as approved by DIR, which set the objectives, scope, and principles that ensure the success of the Incident Management processes.

2.3.1.6 Provide effective and agreed mechanisms for properly complying with the Service Desk policies.

2.3.1.7 Manage all Incidents, Service Requests, etc., from Authorized Users relating to Services, including the following:

2.3.1.7.1 Assigning categorization and prioritization codes.

2.3.1.7.2 Communicating with users, keeping them informed of progress, notifying them of impending actions, obtaining appropriate agreement, and in all ways engaging and communicating with them about Service Provider activities.

2.3.1.7.3 Closing all resolved Incidents, Service Requests, and other calls.

2.3.1.8 Develop and document processes regarding interfaces, interaction, and responsibilities between Level 1 Support personnel, Level 2 Support personnel, and any other internal or external persons or entities that may either submit an Incident or receive an Incident.

2.3.1.9 Utilize the Incident Management System provided by the MSI and integrate with the MSI Service Desk, including tools, technology, processes, and procedures.

2.3.1.10 Analyze Incident trends and recommend and implement actions, with DIR and DIR Customer's approval, to reduce Incidents, including:

2.3.1.10.1 Increase the availability of self-help capability, such as providing on-line FAQs and help documentation for common problems.

2.3.1.10.2 Provide the MSI with information necessary to keep Authorized Users regularly updated with alerts advising of any new or changed information.

2.4 Outreach and Growth

The Service Provider shall promote the Services to public sector entities within the State of Texas; including all potential DIR Customers, specifically state agencies, universities and higher education, counties, and municipalities.
Service Provider shall, at a minimum:

2.4.1.1 Develop and execute against an Outreach Approach, subject to the approval of DIR, that describes how Services are branded and communicated, how stakeholder needs are assessed, what outreach efforts meet those needs, and how satisfaction with Services is measured and improved.

2.4.1.1.1 Update the sales approach annually, subject to DIR approval, to address, at minimum:

1. Methods for communicating available Services.
2. Methods to assess stakeholder needs.

3. Strategies for branding, including: assessment of the existing brand, description of how the brand aligns with the core mission and vision, discussion of obstacles to branding development, details of specific functionality and recommendations, and presentation of a mock-up version of brand and design.
4. Identification of Services and functionality that drive DIR Customer adoption.
5. Plan to measure and track DIR Customer satisfaction and complaints.

2.4.1.2 Provide outreach to current and potential DIR Customers.

2.4.1.2.1 Collaborate with DIR Customers to understand their needs and to promote the benefits of security initiatives.

2.4.1.2.2 Communicate and promote specific service benefits to targeted needs.

2.4.1.2.3 Deliver compelling incentives to DIR Customers to use the Services.

2.4.1.2.4 Build trust through promotion of the benefits, ease of use, security, and privacy.

2.4.1.2.5 Establish an ongoing feedback, response, and resolution process.

2.4.1.3 Facilitate a community where state security personnel are encouraged to share knowledge, ideas, and best practices to collaborate across boundaries.

2.4.1.4 Provide a central repository where users can leverage the power of common solution sets to extend benefits across boundaries, improve overall security posture, share best practices, and enhance existing security solutions.

3 SERVICE MANAGEMENT

3.1 Incident Management

The primary activities of Incident Management include, at a minimum:

1. Incident classification and initial support;
2. Incident investigation and diagnosis;
3. Incident escalation;
4. Incident resolution and recovery; and
5. Incident ownership, monitoring, tracking, and communication.

3.1.1 Requirements

Service Provider shall, at a minimum:

3.1.1.1 Provide Incident Management Services in the form of tier 2 support and tier 3 support. Incident Management is separate and distinct from Security Incident Management.

3.1.1.2 Provide knowledge capture and transfer regarding Incident resolution procedures to support the objective of increasing the number of Incidents capable of being resolved by tier 1 support.

3.1.1.3 Comply with MSI policies and procedures for Incident Management.

3.1.1.4 Coordinate with the MSI to develop and approve Service Provider-related Incident Management content in the MSI-managed SMM.

3.1.1.5 Utilize the Incident Management System provided by the MSI for all information related to an Incident.

3.1.1.6 Provide for training on processes and tools for Incidents and escalations to Service Provider Incident Management staff and other relevant resources involved with responding to Incidents.

3.1.1.7 Resolve Incidents in accordance with the SMM, knowledge database documents, and configuration database(s).

3.1.1.8 Identify and classify Incident Priority and handle according to agreed-upon Incident response procedures and assume end-to-end responsibility.

3.1.1.9 Escalate Incidents in accordance with the SMM, knowledge database documents, and configuration database(s).

3.1.1.10 Provide tier 2 support and tier 3 support, unless tier 3 support is provided by a third-party vendor.

3.1.1.11 Participate in Incident review sessions.

3.1.1.12 Update the progress of an Incident's resolution within the MSI tracking systems through to final closure.

3.1.1.13 Verify that all records (e.g., inventory, asset and configuration management records) are updated to reflect completed and resolved Incidents.

3.1.1.14 Document solutions to resolved Incidents in MSI-managed central knowledge base. Accurately update all information pertinent to trouble ticket including general verbiage, codes, etc.

3.1.1.15 Determine if an Incident should initiate a Problem investigation (e.g., whether preventive action is necessary to avoid Incident recurrence) and, in conjunction with the appropriate support tier, raise a Problem record to initiate action.

3.1.1.16 Conduct follow-up with Customer representative who reported the Incident to verify the Incident was resolved to their satisfaction.

3.1.1.17 Integrate the Service Provider's Incident Management process with the other service management processes, especially Problem Management, Configuration Management, Service Level Management, and Change Management.

3.1.1.18 The Service Provider shall utilize the Incident Management System provided by the MSI and integrate such with their Incident Management processes, providing a level of sophistication that allows for a set of Incident Resolution diagnostics.

3.2 Problem Management

The primary activities of Problem Management include, at a minimum:

1. Problem control;
2. Error control;
3. Proactive prevention of Problems;
4. Identify trends that could result in Incidents or Problems;
5. Perform major Problem reviews; and
6. Provide Problem Management reporting.

3.2.1 Requirements

The Service Provider shall, at a minimum:

3.2.1.1 Provide Problem Management Services in coordination with the MSI Problem Management structure to minimize the adverse impact of Incidents on DIR Customer's business operations.

3.2.1.2 Cooperate with the MSI to provide reactive Problem Management Services by diagnosing and solving Problems in response to one or more Incidents that have been reported through Incident Management.

3.2.1.3 Provide proactive Problem Management to identify and solve Problems and known errors before Incidents occur, including:

3.2.1.3.1 performing predictive analysis activities, where practical, to identify potential future Problems,

3.2.1.3.2 develop recommended mitigation plans, and

3.2.1.3.3 implement approved corrective mitigation actions and processes.

3.2.1.4 Maintain, update, and disseminate information about Problems and the appropriate workarounds and resolutions to reduce the number and impact of Incidents.

3.2.1.5 Provide Problem Management Services for all Problems that are determined to be related to the in-scope Services. Service Provider shall also provide coordination and assistance to Customer and other Service Component Providers in performing their Problem Management functions related to the in-scope Services.

3.2.1.6 Implement resolutions to Problems through the appropriate control procedures, especially Change management, as well as coordinating Problem Management activities with the various teams within Service Provider, Customer, MSI and other Service Component Providers responsible for performing Configuration Management, IT Service Continuity Management, and Service Level management activities.

3.2.1.7 Coordinate with the MSI to develop and implement processes for Problem Management and root cause analysis (RCA) (e.g., events that trigger an RCA).

3.2.1.8 Comply with MSI policies for Problem Management and RCA.

3.2.1.9 Participate in Problem Management review meetings.

3.2.1.10 Use and update the Problem Management knowledge database managed by the MSI.

3.2.1.11 Perform Problem Management activities as set forth in the MSI-managed SMM.

3.2.1.12 Coordinate and take responsibility of Problem Management activities of all Problems that reside in Service Provider's area of responsibility (e.g., detection, logging, RCA, etc.).

3.2.1.13 Conduct proactive trend analysis of Incidents and Problems to identify recurring situations that are or may be indicative of future Problems and points of failure.

3.2.1.14 Develop and recommend corrective actions or solutions to address recurring Incidents and Problems or failures, as well as mitigation strategies and actions to avert potential Problems identified through trend analysis.

3.2.1.15 Identify, develop, document (in the MSI Problem Management tool), and recommend appropriate workarounds for known errors of unresolved Problems and notify Incident Management and all other appropriate Customer stakeholders of its availability, if approved by Customer.

3.2.1.16 Create Request for Change (RFC) documentation with recommended corrective actions to resolve a Problem and submit to Change management for review and approval using the MSI provided tool.

3.3 Information Security Management

Service Provider's delivery of Information Security Management shall be an integral part of the Services and shall assess all security risks associated with the delivery of Services are appropriately identified, evaluated, assessed and appropriate controls are implemented and maintained.

3.3.1 Information Security Management General Requirements

The Service Provider shall, at a minimum:

3.3.1.1 Work with the MSI in support of the overall cybersecurity risk management program.

3.3.1.2 Support the MSI in the development and maintenance of security procedures and Service Responsibility Matrices, physical and logical access strategies and standards

3.3.1.3 Adhere to the Information Security Management processes as defined in the SMM.

3.3.1.4 Work with the MSI to integrate Service Provider's security program with DIR's governance risk and compliance program, including at a minimum Incident recording, CMDB, security exception, security plan submission, risk assessment and in integrating Service Provider's Security tools directly with the MSI as required to support these capabilities.

3.3.1.5 Implement security capabilities as required to achieve compliance with security laws, rules and regulations.

3.3.1.6 Support security evaluations, as directed by DIR, which include conducting internal audits, supporting external audits, conducting self-assessments, and evaluating security Incidents.

3.3.1.7 Support all DIR authorized assessments, develop action plans and resolve deficiencies, vulnerabilities, concerns and recommendations identified within six (6) months of the conclusion of the assessment, as defined in **Attachment 3-C Critical Deliverables**.

3.3.1.8 Meet all Security-related Service Levels as defined in **Exhibit 3 Service Levels**, which are to be agreed to by DIR and Service Provider.

3.3.1.9 As requested, attend and contribute to Security Management and Risk Management meetings.

3.3.1.10 Resolve agreed actions and activities resulting from Security Management meetings.

3.3.1.11 Support MSI and contribute to the creation and maintenance of a Security Plan across the Service Provider's Services

3.3.1.12 Execute Service Provider's Security Plan which is agreed to by DIR and coordinated by the MSI.

3.3.1.13 Ensure that certificates for Service Provider's staff are kept current and report the status to the MSI on a quarterly basis.

3.3.1.14 Provide for vulnerability scans for all Service Provider network assets, which should include scans for all network addresses at least once per year.

3.3.1.15 Provide a forward-looking schedule for the planned Service Provider Security testing, assessments and analysis.

3.3.1.16 In coordination with the MSI, support the evaluation of new technologies/capabilities for improving security and perform activities and/or solutions to address shortfalls in Security.

3.3.1.17 Where investment decisions are required, support the MSI in providing options with associated costs and benefits for DIR review and approval.

3.3.1.18 In coordination and support of the MSI, and as related to the Service Provider's Services, evaluate details of the Security requirements for new IT services, including options for meeting these requirements and any associated costs.

3.3.1.19 Support the MSI and execute processes according to the governance-approved Master Security Baseline Configuration (MSBC).

3.3.1.20 Support and execute quarterly MSBC Health Checks and run scans quarterly that will feed baseline information to the MSI for the MSI to determine the health check of the systems.

3.3.2 Service Provider Staff

The Service Provider shall, at a minimum:

3.3.2.1 Limit access to data to authorized Service Provider personnel only.

3.3.2.2 Service Provider personnel must have received security clearance and successfully complete a background and criminal history investigation prior to performing contract functions or accessing DIR, DIR Customer Facilities, Systems, Networks or Data.

3.3.2.2.1 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.

3.3.2.2.2 Background and criminal history background checks 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 DIR Customers may require additional levels of compliance as per agency regulations and policies.

3.3.2.2.3 Service Provider is responsible for any costs associated with the criminal history background check process.

3.3.2.2.4 Service Provider will establish a process that facilitates the timely submission and resolution of the criminal history background checks, including but not limited to using digital methods to submit necessary criminal history background check requirements.

3.3.2.3 Implement processes and procedures for tracking Clearances for all Service Provider personnel and Third Party Vendors utilizing the Security Clearance Management System provided by the MSI.

3.3.3 Security Incident Management

The Service Provider shall, at a minimum:

3.3.3.1 Support MSI and contribute to the creation of a Security Incident Management Plan across the Service Provider's Services.

3.3.3.1.1 Provide plans and exceptions for all security Incident Management plans including security Incident priority matrix, notification rosters, communications plans, and procedures for managing security Incidents.

3.3.3.1.2 Implement the Service Provider's portion of the Security Incident Management Plan in concert with participation from the MSI and required Service Component Providers and DIR Customer personnel.

3.3.3.1.3 Coordinate Security Incident Management procedures with Major Incident Management procedures.

3.3.3.2 Support the security incident handling and notification processes that follow current NIST guidelines and is defined in the SMM.

3.3.3.3 As required, implement and maintain monitoring and alerting services that integrate into the MSI Incident Management System for automated alert notification.

3.3.3.4 Promptly investigate, document, and report security incidents in accordance with 1 TAC Chapter 202 and the SMM.

3.3.3.5 According to the defined process, promptly communicate and escalate security Incidents to the MSI, Customer, and DIR.

3.3.3.6 Conduct Root Cause Analysis and if necessary, develop and implement formal corrective actions or remediation plans once approved by DIR and the appropriate Customer. Evaluate the analysis and proposed corrective actions to ensure future risks are adequately mitigated.

3.3.3.7 Provide Incident investigation support, and initiate corrective actions to minimize and prevent security breaches.

3.3.4 Physical Security Administration

The Service Provider's shall, at a minimum:

3.3.4.1 Communicate the physical and logical security management processes and procedures to Service Provider's staff.

3.3.4.2 Comply with Service Provider physical and logical security responsibilities.

3.3.4.3 Inform MSI and DIR Customer immediately if Service Provider becomes aware of any vulnerability or weakness in the Services, and recommend a solution or mitigation.

3.3.4.4 Provide near real-time information, to MSI and DIR Customers to identify those physical access rights that should be removed from MSI and DIR Customer Facilities and where, within the Service Provider's scope of responsibilities, initiate the access rights revocation request.

3.3.5 DIR and Customer Sites

Where Service Provider uses or visits locations and facilities at DIR and DIR Customer Sites, Service Provider shall be responsible for the provision of Services related to Customer's security requirements, set in place by DIR Customer to govern the security of the DIR Customer Environment.

Service Provider shall, at a minimum:

3.3.5.1 Ensure compliance with all DIR and DIR Customer security policies, standards and procedures, and all applicable laws and regulations, as they may be revised or updated.

3.3.5.2 Comply with DIR and DIR Customers' policies, including security, data and records management, and electronic records and data archiving.

3.3.5.3 Implement the security-related Services required to protect the confidentiality, integrity, and authenticity of the information stored in or transmitted to or from the DIR Customer environment, in accordance with DIR Customer's security requirements.

3.3.5.4 Integrate Service Provider's Physical Security Administration process with DIR's, DIR Customers,' and Service Component Providers' Physical Security Administration processes, where the processes interact.

3.3.5.5 Where DIR Customer's security requirements do not exist, propose new process and procedures based on industry best practices to DIR Customer for DIR Customer's review, acknowledgement, and approval.

3.3.5.6 Assist in the development of action plans following any Security Incidents within the DIR Customer environment and implement new controls approved by DIR Customer and in the timeline defined by DIR Customer.

3.3.5.7 Maintain all security documentation related to DIR Customer's enterprise security architecture for Equipment, Software, and networks; ensure documentation is available online to Customer 24x7x365.

3.3.5.8 Maintain DIR Data in accordance with DIR Customer's security policies.

3.3.5.9 Establish and maintain safeguards against the unauthorized access, destruction, loss, or alteration of DIR Data in the possession of Service Provider in accordance with DIR Customer's security policies.

3.3.5.10 Participate in Service Delivery to review any Changes to the Equipment, Software, and networks that potentially have security or operational ramifications and modify the Change to remove or reduce the security or operational ramifications.

3.3.6 Other Locations

Service Provider shall, at a minimum:

3.3.6.1 Where Service Provider uses other locations and facilities to support the provision of Services to DIR or DIR Customers, Service Provider's responsibilities shall include the following:

3.3.6.1.1 Provide security processes, facilities, Equipment, and Software that meet or exceed DIR's physical security policies, standards, and procedures. Such

processes and physical attributes will be at a minimum consistent with similar security provisions maintained by large, well-managed sourcing services companies.

3.3.6.2 Upon request, provide DIR, its representative(s), and/or regulatory DIR Customers access to all facilities and assets used in providing the Services for audits, investigations, and compliance reviews.

3.3.6.3 Perform all physical security functions (e.g., identification badge controls and alarm responses) at facilities under Service Provider's control.

3.3.7 Security Assessments

Service Provider shall, at a minimum:

3.3.7.1 DIR may initiate and conduct assessments of Service Provider's security program. 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.

3.3.7.2 DIR, DIR 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) 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.

3.3.8 Assessments

Service Provider shall, at a minimum:

3.3.8.1 DIR may conduct security assessments, including conducting monitoring and testing security programs (e.g., Controlled Penetration Tests), conducting risk assessments and performing Security Design Reviews, (the "Assessment(s)") of all or any portion of the Services in order to evaluate such Security Program and determine whether the Security Program meets or exceeds the Standard of Due Care.

3.3.8.2 Assessments of the Security Program may be conducted by DIR or, at DIR's sole discretion, a third-party security assessment vendor (the "Security Assessment Company").

3.3.8.3 The Service Provider shall cooperate fully with DIR and/or the Security Assessment Company and provide reasonable access to any premises, equipment, personnel or documents and provide any assistance required by DIR and/or the Security Assessment Company to conduct the Assessment; however, DIR and the Security Assessment Company shall not have access to Service Provider proprietary information where it is not relevant to the Assessment, and shall further not have access to confidential or proprietary information of other customers of Service Provider than DIR Customers.

3.3.8.4 Under no circumstances will Service Provider attempt to persuade or control or otherwise influence the Security Assessment Company in the determination of its findings. The Assessment shall be conducted so as not to unreasonably disrupt Service Provider's operations under this Agreement.

3.3.8.5 Within fifteen (15) days of an Assessment Notice Date, DIR and Service Provider will meet to jointly review the relevant Assessment report and if such report concludes that the Security Program does not meet or exceed the Standard of Due Care, then within thirty (30) days after the applicable Assessment Notice Date, the Service Provider and the MSI shall develop and agree upon an action plan to promptly address and resolve any deficiencies, vulnerabilities, concerns and/or recommendations identified in such report, consistent with the Service Provider's obligations as set forth in the Agreement.

3.4 Request Management and Fulfillment

Service Provider shall be responsible for the fulfillment of Service Requests in compliance with processes in the SMM.

3.4.1 Requirements

The Service Provider shall, at a minimum:

3.4.1.1 Actively participate with the MSI to develop and document processes.

3.4.1.2 Actively cooperate with the MSI in implementing and maintaining Request Management and Fulfillment processes that are flexible and facilitate effective communication and coordination across all functional areas.

3.4.1.3 Actively cooperate in information exchange between and among the Service Provider, the MSI, other Service Component Provider(s), DIR, and Customer to improve end-to-end Request Management.

3.4.1.4 Integrate the Service Provider's Request Management process with the MSI's Request Management process and systems, where the processes interact.

3.4.1.5 Facilitate the automation or mechanization of Service Requests between Service Provider and other Service Component Provider(s) systems.

3.4.1.6 Facilitate the transparency of Request Management through appropriate processes to provide a complete audit trail for the MSI to meet DIR and Customer legislative and policy requirements.

3.4.1.7 Actively support the MSI as appropriate to ensure the proper exercise of Request Management activities across all functions and organizations that provide Services to Customers.

3.4.1.8 Communicate and coordinate the Request Management processes and policies within Service Provider's organization.

3.4.1.9 Actively participate in defining Request Management processes, as approved by DIR, to ensure the success of Request Management.

3.4.1.10 Provide effective and agreed mechanisms for properly complying with the Request Management Policies.

3.4.1.11 Actively participate in developing and establishing Request for Solution processes and appropriate mechanisms to support rapid proposal development that provides a level of accuracy for budgetary information without requiring a full solution.

3.4.1.12 Actively support the MSI in establishing processes and workflow for the proper routing of Service Requests.

3.4.1.13 Actively participate in Service Request tracking efforts, and provide and maintain regular communications between all parties and Authorized Users through Request fulfillment.

3.4.1.14 Manage the effective execution of Request Management for Service Provider to achieve its primary purpose to fulfill service requests within the agreed Service Levels and promote Customer and Authorized User satisfaction.

3.4.1.15 Support the MSI to ensure that detailed audit trail information is recorded of all activity that creates, changes, or deletes data and user access to systems that contain DIR and Customer data.

3.4.1.16 Engage in effective Request Management governance process to support the MSI in ensuring the following:

3.4.1.16.1 Clearly define and document the type of Service Requests that will be handled within the Request Management process so that all parties are clear on the scope of Service Requests and the Request Management process.

3.4.1.16.2 Establish and continually maintain definitions of all Services, including: descriptions, Services that will be standardized, Services that require custom solutions, and Services that can be requested through each medium (e.g., Service Desk, Portal, Service Catalog, Request for Service).

3.4.1.16.3 Establish and continually maintain Authorized User lists on who is authorized to make Service Requests and type of requests they are entitled to make.

3.4.1.16.4 Communication to DIR and Customers on the definition of Services, the Request Management processes, and changes thereto.

3.4.1.16.5 Regular training for Authorized Users on Request Management processes, Service definitions, and request mediums.

3.4.1.16.6 Regular collection of feedback from Authorized Users on the effectiveness of Request Management and engage in activities to improve process and service.

3.4.1.17 Support multiple mediums for accepting Service Requests, including the Service Desk, Portal, and Service Catalog.

3.4.1.18 Support the use of online self-service to allow Authorized Users to enter Service Requests from a pre-defined list of options.

3.4.1.19 Support the provision for real-time visibility of data records associated with Service Requests.

3.4.1.20 Update required information on Service Requests within negotiated timeframes to support an up-to-date accurate view of Service Requests.

3.4.1.21 Ensure proper approval, including financial authority, or the Service Request through automated means (where practical) prior to Service Request fulfillment.

3.4.1.22 Provide and maintain regular communications between all parties and Authorized Users as required until Service Request completion and document the communications in compliance with the Request Management processes.

3.4.1.23 The communications frequency shall be determined by the severity of the request and in compliance with the SMM.

3.4.1.24 Keep Customer and MSI informed of any issues with the completion of Service Requests and status changes throughout the Service Request lifecycle and in accordance with agreed Service Levels.

3.4.1.25 Provide anticipated completion times for active Service Requests and update notification systems as required in the SMM to keep Customers and Authorized Users informed in compliance with established Service Levels per **Exhibit 3, Service Levels**.

3.4.1.26 Support the MSI to ensure consistent ownership of the Service Request from recording to completion.

3.4.1.27 Close Service Requests, in compliance with the SMM, after receiving confirmation from the requesting Authorized User or Service Provider support personnel that the Service Request has been completed.

3.4.1.28 Track the progress of fulfillment efforts and the status of all Service Requests, including:

3.4.1.28.1 Review the proposed fulfillment time for each Service Request with the appropriate party and update the status accordingly.

3.4.1.28.2 Provide regular updates on the status of all Service Requests within designated timeframes.

3.4.1.28.3 Coordinate Service Request tracking efforts and provide and maintain regular communications, per the SMM, between all parties and Authorized Users until Service Request completion.

3.4.1.28.4 Keep the Customer and Authorized User informed of changes in Service Request status throughout the Service Request lifecycle in compliance with agreed Service Levels.

3.4.1.28.5 Keep Customer informed of anticipated Service Request completion times for active Service Requests.

3.4.1.28.6 When a Service Request cannot be completed in the committed timeframe, provide a revised completion time or request a meeting with the Authorized User to determine a new timeframe.

3.4.1.28.7 Track all Service Request completion against the original committed timeframe, regardless of any revisions.

3.4.1.29 Utilize the Request Management System provided by the MSI for all Request Management and Fulfillment activities.

3.4.1.30 Provide for timely receipt and processing of all requests within designated timeframes from the Request Management System.

3.4.1.31 Utilize and update the Request Management System with all relevant information relating to a Service Request.

3.5 Change Management

The Change Management process includes the following process steps and may be updated from time to time:

1. Request for Change (RFC);
2. Recording/tracking;
3. Prioritization;
4. Responsibility assignment;
5. Impact/risk assessment;
6. Approved changes schedule management;
7. Measuring effectiveness of a Change;
8. Review/approval;
9. Implementation;
10. Verification;
11. Closure; and
12. Change Advisory Board (CAB) execution.

3.5.1 Requirements

The Service Provider shall, at a minimum:

3.5.1.1 Service Provider shall perform Change Management Services utilizing standardized methods and procedures as defined in the SMM to provide efficient and prompt handling of all Changes.

3.5.1.2 Service Provider shall assist Customer in creating the schedule for any Changes and implementing such Changes.

3.5.1.3 Assist Customer and MSI to refine and improve upon Change Management processes and training requirements including CAB composition, activities, and the financial, technical, and business approval authorities appropriate to Customer requirements.

3.5.1.4 Comply with MSI Change Management processes and training requirements.

3.5.1.5 Review and approve refinements to Change Management processes and training requirements.

3.5.1.6 Provide necessary information to Customer and MSI to assist in documenting all Request for Change's (RFCs), which could include Change cost, risk impact assessment, and system(s) security considerations.

3.5.1.7 Coordinate with Customer to assist in the development of a schedule of planned approved Changes.

3.5.1.8 Perform maintenance during regular Maintenance Periods as defined in the SMM, or as scheduled in advance with the approval of Customer.

3.5.1.9 Provide Change documentation, as required, to the MSI, including proposed metrics on how effectiveness of the Change might be measured.

3.5.1.10 As requested, participate in traditional or digital CAB meetings and workflow to review planned Changes and results of Changes made.

3.5.1.11 Utilize the Change Management System, tools, and processes of the MSI for the efficient and effective handling of all Changes, including the CAB, subject to approval from Customer, in a way that minimizes risk exposure and maximizes availability of the Services.

3.6 Asset Inventory and Management

Asset Inventory and Management will provide an inventory of the IT infrastructure managed by the Service Provider. The MSI consolidates information from multiple Service Provider Asset Inventory and Management Databases that contain details of Equipment, Software, and similar IT service items (collectively referred to as Configuration Items or CIs) used in the provision, support, and management of IT services.

3.6.1 Requirements

The Service Provider shall, at a minimum:

3.6.1.1 Actively participate with the MSI to develop and document Asset Inventory and Management processes, as approved by DIR, that document the objectives, scope, and principles that ensure the success of the Asset Inventory and Management processes.

3.6.1.2 Integrate Service Provider Asset Inventory and Management process with the MSI's Asset Inventory and Management process and systems, including providing Service Provider asset data electronically to MSI's Asset Inventory and Management System (AIMS) in the agreed data format.

3.6.1.3 Communicate and coordinate the Asset Inventory and Management processes and policies within Service Provider's organization.

3.6.1.4 Actively cooperate in information exchange between and among the Service Component Provider(s), MSI, DIR and Customer to improve end-to-end Asset Inventory and Management.

3.6.1.5 Support the MSI to provide a complete Asset Inventory and Management audit trail to meet DIR and Customer legislative and policy requirements.

3.6.1.6 Conform operations to policies and procedures that set the objectives, scope, and principles that ensure the success of the Asset Inventory and Management process.

3.6.1.7 Support the MSI in establishing categorization and classification structures to support the proper documentation and maintenance of CIs.

3.6.1.8 Use the Asset Inventory and Management process to identify, control, maintain, and verify the CIs approved by the MSI as comprising the Equipment, Software, and Applications to provide the Services.

3.6.1.9 Record the CI information for Equipment, Applications, Software and Services.

3.6.1.10 Verify that all CIs for the Equipment, Applications, Software, and Services are incorporated into the AIMS.

3.6.1.11 Utilize the AIMS provided by the MSI as the single source of information regarding all CIs within Service Provider scope.

3.6.1.12 Ensure that all CI data related to the Services resides in the AIMS.

3.6.1.13 Integrate the Service Provider's other systems, including all appropriate and required licenses and/or interfaces with the MSI's AIMS.

3.6.1.13.1 Where Service Provider has an internal asset inventory system or database, integrate that system or database with the MSI AIMS as required.

3.6.1.13.2 Provide customization as required to enable the Asset Inventory and Management processes as defined in the SMM.

3.6.1.13.3 Automate processes, discovery tools, inventory and validation tools, enterprise systems and network management tools, etc. to provide electronic Asset Inventory and Management data as required to the MSI.

3.6.1.14 Comply with existing and established SMM processes.

3.7 Software License Management

3.7.1 Software License Renewal Management

The Service Provider shall, at a minimum:

3.7.1.1 Supporting the MSI in tracking, monitoring, and reporting the software renewal process to ensure compliance with software agreements and continued operation of Services.

3.7.1.2 Comply with the Software License Renewal Management processes, as defined in the SMM.

3.7.1.3 Support Service Requests and Change Requests as appropriate for all renewals and update as needed to reflect the status of each renewal as per the timing and lifecycle process defined in the SMM (e.g., Software expiring in May should be logged as a CRQ in January, 120 days prior to the expiration date).

3.7.1.3.1 Service Provider will update the contract data in the approved Software License Renewal System, coordinate with the Customer and MSI to obtain renewal approvals, execute the procurement tasks to renew the software license, install the renewed keys and software, update the Change Request and Contracts data, and log the renewed software keys in the Software License Renewal System as per the process defined in the SMM.

3.7.1.4 In conjunction with the MSI, monitor Software License Renewal progress and SLA achievement.

3.7.1.5 Support the MSI to ensure the requests and Change Requests are completed and closed upon renewal completion.

3.7.2 Software License Compliance Management

The Service Provider shall, at a minimum:

3.7.2.1 Support the MSI to determine the compliance position, monitor and report the software compliance management process to ensure compliance with agreements and reduce operating risk in the environment.

3.7.2.2 For Service Provider provided and managed software, support and execute assigned Software License Compliance Management activities as defined in the SMM.

3.7.2.2.1 For DIR and Customer-retained Software, track and maintain the applicable licensing and use information received from Customers.

3.7.2.2.2 Utilize tools, such as an enterprise management system and remote monitoring agents, to assist in monitoring efforts, subject to DIR's approval of all such tools.

1. Monitor the Equipment for the presence of any unauthorized or non-standard Software.
2. Define and check for particular Software signatures.
3. Monitor the use of Software developed by the Service Provider application development groups.
4. Check the presence and version of Software installed on a particular device and record in the MSI Asset Inventory and Management system.

3.7.2.2.3 Provide reporting of license information and compliance to the MSI, at least quarterly or as directed by DIR.

3.7.2.2.4 Store and track Software license agreements and associated license keys, including processes and procedures for renewals.

3.7.2.2.5 Track license counts and associations within the CMDB.

3.7.2.2.6 Collect and provide the Proof of Entitlement (POE) data to the MSI.

3.7.2.2.7 Support the MSI to collect and normalize software titles to standard names.

3.7.2.2.8 Support the MSI to review the Software License Compliance position and determine appropriate remediation.

3.7.2.2.9 Support assigned actions through the Incident, Request, Change, and Project processes for any reported non-compliance of software purchased versus software installed.

3.7.2.2.10 Support and provide clarifications about information presented in the Compliance Report to eliminate discrepancies.

3.7.2.3 Support the use of Service Provider provided and managed Software to maintain strict compliance, including but not limited to:

3.7.2.3.1 Immediately notify and advise MSI of all Software license compliance issues associated with Services.

3.7.2.3.2 Support in the tracking, management and implementation of security certificates used to secure confidential sessions (e.g., SSL) for Internet and Intranet transactions and communications, including processes and procedures for renewals, as required by DIR, Customers, or MSI.

3.7.2.4 Support the MSI to confirm the presence and version of Software installed on a particular device and that those attributes are recorded in the MSI Asset Inventory and Management system.

3.7.2.5 Support the MSI in reporting of license information and compliance to DIR.

3.7.3 Patch Management

The Service Provider shall, at a minimum:

3.7.3.1 Be responsible for patch deployment and control of the software and devices under management.

3.7.3.2 Be responsible for participating in Customer Change Management processes to deploy patches on a regular basis.

3.7.3.3 Participate in and follow the agreed upon patch rating process.

3.7.3.4 Deploy patches to servers and clients per Customer's policies and ensure compliance as required. Use the Customer-approved central deployment tool, as applicable and mutually agreed upon.

3.7.3.5 Provide and apply patches to devices within the timeframe guidelines in accordance with Customer's security policies.

3.7.3.6 Adhere to Customer's security configuration management.

3.7.3.7 Communicate with and/or alert the Customer IT Security team when patches are not installed within the designated timeframe.

3.7.3.8 Integrate and have the ability to export patch data associated will all Customer devices.

3.8 Configuration Management

Configuration Management will provide a logical model of the IT infrastructure managed by the Service Provider to identify, control, maintain, and verify information related to all Configuration Items that support the Service Provider's Services. The MSI consolidates information from multiple Service Component Provider Configuration Management Databases (CMDBs) that contain details of Configuration Items (CIs) used in the provision, support, and management of IT services.

3.8.1 Requirements

The Service Provider shall, at a minimum:

3.8.1.1 Actively participate with the MSI to develop and document Configuration Management processes, as approved by DIR, that document the objectives, scope, and principles that ensure the success of the Configuration Management processes.

3.8.1.2 Integrate Service Provider Configuration Management process with the MSI's Configuration Management process and systems, including providing Service Provider Configuration data electronically to MSI's CMS / CMDB in the agreed data format.

3.8.1.3 Communicate and coordinate the Configuration Management processes and policies within Service Provider's organization.

3.8.1.4 Actively cooperate in information exchange between and among the Service Component Provider(s), MSI, DIR and Customer to improve end-to-end Configuration Management.

3.8.1.5 Support the MSI to provide a complete Configuration Management audit trail to meet DIR and Customer legislative and policy requirements.

3.8.1.6 Conform operations to policies and procedures that set the objectives, scope, and principles that ensure the success of the Configuration Management process.

3.8.1.7 Support the MSI in establishing categorization and classification structures to support the proper documentation and maintenance of CIs.

3.8.1.8 Use the Configuration Management process to identify, control, maintain, and verify the CIs approved by the MSI as comprising the Equipment, Software, and Applications to provide the Services.

3.8.1.9 Record the CI information and relationships to applications, software, services, and equipment.

3.8.1.10 Verify that all CIs for the Equipment, Software, and Services are incorporated into the CMDB.

3.8.1.11 Utilize the CMDB provided by the MSI as the single source of information regarding all CIs within Service Provider scope.

3.8.1.12 Ensure that all configuration data related to the Services resides in the CMDB.

3.8.1.13 Integrate the Service Provider's other systems, including all appropriate and required licenses and/or interfaces with the MSI's Configuration Management System(CMS).

3.8.1.13.1 Where Service Provider has an internal CMS, integrate that system with the MSI CMS as required.

3.8.1.13.2 Where Service Provider has an internal CMDB integrate that database with the MSI CMDB.

3.8.1.13.3 Provide customization as required to enable the Configuration Management processes as defined in the SMM.

3.8.1.13.4 Automate processes, discovery tools, inventory and validation tools, enterprise systems and network management tools, etc. to provide electronic asset and configuration management data as required to the MSI.

3.8.1.14 Comply with existing and established SMM processes.

3.9 IT Service Continuity Management

Service Provider is responsible for maintaining an IT Service Continuity Management (ITSCM) plan for its own internal staff and systems to respond to an emergency and continue to provide Services to DIR and Customers.

3.9.1 General Requirements

The Service Provider shall, at a minimum:

3.9.1.1 Develop, maintain, and test Disaster Recovery Plans (DRPs) and Technical Recovery Guides (TRGs) as defined in the SMM for the Systems, Software, and Equipment used by Service Provider to provide the Services, including those provided at the Consolidated Data Centers, Customer Service Location, or other Service Provider Facilities.

3.9.1.1.1 The DRPs and TRGs should comply with all applicable Federal and State requirements.

3.9.1.2 In the event of a disaster, recover and support affected Systems, Software, and Equipment at the designated recovery location according to the agreed Recovery Time Objective (RTO) and Recovery Point Objective (RPO) in compliance with the Service Levels defined in **Exhibit 3**.

3.9.1.3 Coordinate Service Provider's ITSCM plan with MSI ITSCM plans and Customer Business Continuity Plan (BCPs) to ensure Customers can resume regular business functions in the event of a Disaster or significant event affecting the Systems, Software, and Equipment used by Service Provider to provide the Services.

3.9.1.4 In the event of a service disruption, coordinate all ITSCM efforts to ensure smooth and efficient resumption of Services.

3.9.2 Crisis Management

Crisis Management may be necessary, depending on the type of business or geographic location where Services are being performed, in the event of hurricanes, tornados, riots, terrorist threats, etc. The Service Provider shall, at a minimum:

3.9.2.1 Following MSI, DIR, and Customer notification processes for any crisis event occurring in or relating to a Service Provider Facility, DIR Facility, or other facilities managed by Service Provider in connection with the Services.

3.9.2.2 Following statewide notification pyramid alert support as documented in the applicable business continuity plan.

3.9.2.3 Coordinate with MSI, DIR, and Customers requirements for Services that are critical to designated Customer emergency management responsibilities.

3.9.2.4 Coordinate with MSI, DIR, and Customer regarding variances in Services as a result of Crisis Management in compliance with all SMM procedures.

3.10 Project Management

Project Management provides a way to execute and manage projects with the goal of delivering projects from request through completion, meeting Customer requirements in terms of timing, quality, and cost.

3.10.1 Requirements

The Service Provider shall, at a minimum:

3.10.1.1 Be responsible for executing and project managing projects related to the Service Provider's Services.

3.10.1.2 Conform Service Provider operations to MSI-defined policies and procedures to ensure the success of the Project Management process.

3.10.1.3 Use the MSI provided Project and Program Management (PPM) system as the single source of project management and information regarding all projects and programs.

3.10.1.4 Ensure that all Service Provider Project Management data resides in the PPM system.

3.10.1.5 Execute projects according to the approved Program Management and Project Management methodology as defined in the SMM.

3.11 Release Management

The purpose of Release Management is to build, test and deliver specified Services that will accomplish the stakeholders' requirements and deliver the intended objectives.

3.11.1 Requirements

The Service Provider shall, at a minimum:

3.11.1.1 Work with the MSI and other Service Component Providers(s) to develop and establish a Release and distribution process so that each change to Service Provided

Services is controlled, tested, traceable, authorized, and implemented in a structured manner.

3.11.1.2 Conform Service Provider operations to the agreed Release policies, processes and procedures as defined in the SMM.

3.11.1.3 Execute releases according to the approved Release Management methodology as defined in the SMM.

3.11.1.4 Use the MSI provided Release Management System as the single source of Release Management and information regarding all Service Provider Releases.

4 BUSINESS MANAGEMENT

4.1 Operational Intelligence

Service Provider shall provide the data and/or reports to the MSI for report creation and posting via the MSI-managed Operational Intelligence System and Portal as specified in **Exhibit 13-A Description of Reports**. Service Level reports are defined in **Exhibit 3 Service Levels**, and operational reports are defined in **Exhibit 13 Reports**.

4.1.1 Requirements

The Service Provider shall, at a minimum:

4.1.1.1 For core Services, provide online reporting capability with near real-time data for use by Customers in the generation of sophisticated, custom reports.

4.1.1.1.1 Coordinate with the MSI to provide single sign-on access from the MSI Portal to Service Provider's reports.

4.1.1.2 As appropriate, provide near real-time feeds to the MSI's Portal from any Service Provider's Security Dashboard per **Exhibit 13 Reports**.

4.1.1.3 Provide on-time, monthly service-level performance data against each Service Level requirement, via the MSI-managed management tool.

4.1.1.4 Provide mutually agreed to reports and data to the MSI to enable invoice reconciliation.

4.1.1.5 Coordinate with the MSI and provide data to support the creation of integrated Service Provider performance dashboards. Dashboard data should support:

4.1.1.5.1 Near real-time health dashboards for any Systems managed by Service Provider highlighting status of health metrics as defined by Customer.

4.1.1.5.2 Report monthly, quarterly, and annually in the Security Dashboard on the deployment of Tools and procedures to the Customer Environment.

4.1.1.6 The Service Provider shall be responsible for using DIR's security governance, risk and compliance system to provide information relevant to the service offering, including but not limited to risk assessments, Incident reporting, and security plan development.

4.1.1.7 As required, collaborate with other Texas.gov Service Component Providers, to include sharing reports and information via the MSI Portal or other mutually agreed upon mechanism as appropriate to ensure effective Service delivery.

4.1.1.8 Support integration of applicable security Service solutions, in which data from multiple sources (e.g., scan results, multiple IDS platforms/IPS devices, and MDS devices) are incorporated and integrated into the Service.

4.1.1.9 Provide ad hoc and summary Security Incident Reports to DIR OCISO using security systems and data generated in accordance with the format and content of the then current version of 1 TAC Chapter 202.

4.2 Service Level Management

Service Level Management includes the activities associated with managing and reporting attainment of Service Level performance, deliverable commitments, and customer satisfaction.

4.2.1 Requirements

The Service Provider shall, at a minimum:

4.2.1.1 Provide accurate SLA data to the MSI timely, as defined in **Exhibit 3 Service Levels**, and the SMM.

4.2.1.2 When SLAs fail to meet minimum, or expected service level targets, implement Service Level Improvement Plans, as described in the SMM.

4.2.1.3 Analyze Customer Scorecard feedback to understand Customer reporting issues and develop and execute issue resolutions.

4.2.1.3.1 Collate security information from End Users provided to Service Provider (e.g., captured in Service Desk surveys, feedback through emails) regarding suggested improvements to the Security Services.

4.2.1.3.2 Develop an action plan to address suggested improvements to the Security Services identified by Service Provider and Customer, including the following:

1. Provide the action plan to Customer for review.
2. Implement Customer-approved action plans.
3. Report in the Security Dashboard on progress and improvements made on approved action plans.

4.2.1.4 Summarize and report on plans and activities that affect the overall Services to MSI and DIR governance boards.

4.3 IT Financial Management

Service Provider must provide IT Financial Management Services as described in **Exhibit 4**.

4.3.1 Requirements

The Service Provider shall, at a minimum:

4.3.1.1 Actively work with the MSI to develop and document IT Financial Management processes.

4.3.1.2 Actively cooperate in information exchange between and among the MSI, DIR, and Customer to improve end-to-end IT Financial Management.

4.3.1.3 Facilitate the transparency of IT Financial Management through appropriate processes to provide a complete audit trail for the MSI to meet legislative and policy requirements.

4.3.1.4 Integrate Service Provider IT Financial Management process and system with the MSI's IT Financial Management process and system, where the processes interact, and as agreed to with DIR and the MSI.

4.3.1.5 Actively support the MSI to assure the proper application of IT Financial Management across all functions and organizations that provide services to Customers.

4.3.1.6 Communicate and coordinate the IT Financial Management processes and policies within Service Provider's own organization.

4.3.1.7 Utilize the IT Financial System provided by the MSI such that it serves as the single source of information regarding all IT Financial Information for Services within Service Provider scope.

4.3.1.8 Integrate Service Providers' systems and chargeback data with the MSI IT Financial System, including providing all appropriate and required licenses and/or interfaces.

4.3.1.9 Provide sufficient data and detail to support DIR and Customers State and Federal funding accounting, grant, and audit requirements.

4.3.1.10 Collect, aggregate, and provide billing, service provisioning, and service metric information to the MSI as required.

4.3.1.11 Identify unique Customer account identifiers to identify Applications and other services information as required.

4.3.1.12 Provide the MSI with monthly invoice data required for the MSI to render the Service Provider statement of Services.

4.3.1.12.1 Support all charges with detailed invoice data as required in **Exhibit 4-F Form of Invoice**, and supporting utilization data at the Customer, Resource Unit, Charge Category (e.g., Programs, Divisions, Organization Units) as required by the MSI.

4.3.1.13 Actively participate in developing and maintaining the processes for the resolution of invoice disputes within designated timeframes.

4.3.1.14 Provide effective and agreed mechanisms for crediting Customers as appropriate.

4.3.1.15 Effectively execute the processes to record, track, and manage incidents of invoice disputes.

4.3.1.16 Research and review invoice disputes for completeness and supporting data accuracy, and, when necessary, request clarifying data from Customer.

4.3.1.17 Support and initiate additional treatment of invoice disputes to facilitate resolution within designated timeframes.

4.3.1.18 Ensure that incidents of invoice disputes are continually updated, at a minimum on a weekly basis.

4.3.1.19 Keep the MSI informed of activity and anticipated resolution times for active incidents of invoice disputes.

4.3.1.20 Allow DIR to monitor and validate invoice dispute process on an ongoing basis.

4.3.1.21 Provide a process for escalating to Service Provider management incidents of invoice disputes not resolved within the time frames established within DIR policies.

4.4 Capacity Management

Capacity Management assesses the current operations and future demands, pre-empting performance issues by taking the necessary actions before they occur.

4.4.1 Requirements

The Service Provider shall, at a minimum:

4.4.1.1 Integrate Service Provider Capacity Management process and agreed data with the MSI's Capacity Management process and systems, including providing Service Provider Capacity data electronically to MSI's Capacity Management System in the agreed data format.

4.4.1.2 Communicate and coordinate the Capacity Management processes and policies within Service Provider's organization.

4.4.1.3 Actively cooperate in information exchange between and among the Service Component Provider(s), MSI, DIR and Customer to improve end-to-end Capacity Management.

4.4.1.4 Provide the means to automatically aggregate resource and system performance, system utilization, capacity limits for Service Provider Services.

4.4.1.5 Provide the means to automatically calculate and forecast Service Provider Services capacity requirements through trending of collected data anticipating capacity needs.

4.4.1.6 In an automated manner, aggregate capacity information including current capacity and utilization, trends, issues and actions at the Customer and Services level.

4.4.1.7 Initiate Incident Management, Problem Management or Request Management activities as needed to address Capacity Management issues and trends.

4.4.1.8 Action and track agreed capacity mitigations through associated Incidents, service requests, changes or projects using the MSI provided systems.

4.4.1.9 Participate and contribute to Capacity Management meetings.

4.4.1.10 Incorporate appropriate capacity modeling to extrapolate forecasts of growth and other changes in response to projected Customer business and operational needs.

4.4.1.11 Provide meaningful Capacity Planning input to the MSI-coordinated Capacity Plan.

4.4.1.12 Provide meaningful Capacity Planning input to the Technology Plan in support of requirements for long-range planning.

4.4.1.13 Provide meaningful Capacity Planning input to the Refresh Plan in support of Refresh and Technical Currency.