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 2.1.2

Statement of Work

Cross Functional Services

January 30, 2017

Table of Contents

THIS IS EXHIBIT 2.1.2 – CROSS-FUNCTIONAL SERVICES STATEMENT OF WORK FOR MANAGED APPLICATION SERVICES TO THE AGREEMENT BETWEEN DIR AND SERVICE PROVIDER.

1.0 Managed Application Services – Cross Functional Document

1.1 Document Overview

This document contains Service Management categories of responsibilities that will apply to the delivery of services defined in **Exhibit 2.7.1**, **Exhibit 2.7.2,** and **Exhibit 2.7.3** for Managed Application Services (e.g. – Application Development, Application Maintenance, and Rate Card Resources).

1.2 Designation of Responsibilities

The designated roles and responsibilities in Section 2 of this Exhibit 2.1.2 are the typical expectations for the Service Provider and Customer. Adjustments may occur when the Service Provider is engaged by a Customer to propose or deliver services.

The responsibility descriptions may reference the MSI provider for the DIR DCS program. The DCS MSI role is fully described in DIR Contract DIR-DCS-MSI-MSA-001, **Exhibit 2.1** – Multisourcing Service Integrator located on the DIR website: http://dir.texas.gov/View-Search/Contracts-Detail.aspx?contractnumber=DIR-DCS-MSI-MSA-001&keyword=dir-dcs-msi-msa-001

1.3 Overview of Responsibilities by MAS Category

The table below provides a high level view of the applicability of cross-functional responsibilities by MAS Category (Application Development, Application Maintenance, and Rate Card Resources).

Table 1. Responsibilities by MAS Category

	MAS Category		
Cross Functional Area	Application Development Services	Application Maintenance Services	Rate Card Resources
Service Desk Management	X	X	X
Incident Management		X	
Problem Management	X	X	
Service Request Closure	X	X	X
Configuration Management	X	X	
Change Management	X	X	
Release Management	X	X	
Production Deployment Support	X	X	

Service Continuity Management	X	X	
Crisis Management		X	
IT Security Management	X	X	
Monitoring, Reporting and Review	X	X	X
Availability Management	X	X	
Capacity Management	X	X	
Technology Refreshment and Replenishment		X	
Performance Management	X	X	X
License Management	X	X	
IT Financial Management	X	X	X

2.0 Service Descriptions – Cross Functional Services

2.1 Roles and Responsibilities

2.1.1 Service Desk

Service Provider Service Desk shall provide a single point of contact for the MSI 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 STC Customers' Service Component-related Services.

Service Provider responsibilities include:

1. Actively participate in work with the MSI to develop and document processes.
2. Integrate Service Provider Service Desk process with the MSI's Services Desk process, where the processes interact.
3. Integrate Service Provider Service Desk process with the other Service Management processes, especially Incident Management, Problem Management, Change Management, Configuration Management, and Service Request Management.
4. Actively support the MSI to assure the proper application of Service Desk across all functions and organizations that provide services to STC Customers.

5. Communicate and coordinate the Service Desk processes and policies within Service Provider own organization, and as appropriate to other DCS Service Providers associated with Services.
6. Actively participate in defining Service Desk Policies and procedures, as approved by DIR, which set the objectives, scope and principals that will ensure the success of the Incident Management processes.
    6.1. Provide effective and agreed mechanisms for properly complying with the Service Desk Policies.
7. Provide support to the MSI on both a reactive and a proactive basis, and for both in-bound and out-bound support.
8. Manage all Incidents and Service Requests from Authorized Users relating to Services, including:
    8.1. Communicating with MSI and users as requested, 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.
    8.2. Providing closure information to the MSI for all resolved Incidents, Service Requests and other calls.
9. All communications, whether spoken or written, shall be clearly understandable to the MSI.
10. Seamlessly integrate the Service Desk, including tools, technology, processes, and procedures, with the MSI.
11. Analyze Incident trends, and recommend and implement actions, with DIR and STC Customer's approval, to reduce Incidents, including:
    11.1. Increase the availability of self-help capability, such as through providing on-line FAQs and help documentation for common problems.
    11.2. Provide the MSI with information necessary to keep Authorized Users regularly updated with alerts advising of any new or changed information.

Additional Responsibilities for Application Development Service Desk and Application Maintenance Service Desk

Service Provider responsibilities include:

12. Provide support to Authorized Users on both a reactive and a proactive basis, and for both in-bound and out-bound support.
    12.1. Provide processes and procedures to handle designation and establishment of Authorized User rights.
    12.2. Track and manage the rights associated with individual Authorized Users.
13. Manage all Incidents and/or Service Requests from Authorized Users relating to Services, including:
    13.1. Logging all relevant details.
    13.2. Providing first-line investigation and diagnosis.
    13.3. Resolving those as possible.
    13.4. Escalating those that cannot be resolved within agreed timescales.
    13.5. Communicating with users as requested, 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.
    13.6. Making appropriate updates to the CMS in compliance with Configuration Management processes.

14. Ensuring staffing levels and work allocation remains appropriate to handle incident volumes and incident response targets.

15. Ensure that the Service Desk is available at all times (i.e. 24 hours a day, 365 days a year).

16. Provide an effective means of using industry recognized methods to determine, measure and monitor staffing levels, requirements and allocations, including the use of the following considerations:

    16.1. Customer service expectations.

    16.2. DIR and STC Customer business requirements.

    16.3. Size, relative age, design and complexity of the IT Infrastructure (e.g. the number and type of incidents, the extent of customized versus standard deployments).

    16.4. The number of STC Customers and Authorized Users to support, and associated factors such as number of customers, language requirements and skill level.

    16.5. Incident and Service Request types, including duration of time required for call types, local or external expertise required, the volume and types of incidents and Service Requests.

    16.6. The period of support cover required, based on hours covered, out-of-hours support requirements, time zones to be covered, locations to be supported, workload pattern of requests, and the service level targets in place.

    16.7. The type of response required (e.g. telephone, email, fax, voicemail, physical).

    16.8. The level of training required.

    16.9. The support technologies available (e.g. phone systems, remote support tools, etc.).

    16.10. The existing skill levels of staff.

    16.11. The processes and procedures in use.

17. Communicate to Authorized Users in English, using terms that are clearly understood by the Authorized Users and consistent with those used by DIR and STC Customers.

    17.1. All communications, whether spoken or written, shall be clearly understandable to the Authorized User.

18. Seamlessly integrate the Service Desk, including tools, technology and processes, with DIR and STC Customer's Service Desk(s).

19. The Service Desk will be located in an off-site location from DIR (approved by DIR), except for temporary periods where:

    19.1. Calls are overflowed from one team within the Service Desk to another to handle major outages and business releases.

    19.2. Calls that overflow to a different team within the Service Desk are handled by Service Desk personnel who have been trained and are knowledgeable on the DIR and STC Customer environment.

    19.3. Where more than one site is proposed for the delivery of Service Desk Services, any switching between the sites must be transparent to Authorized Users.

20. Provide Service Provider Service Desk personnel that are trained for the following:

    20.1. Possess the appropriate competencies to provide Service Desk Services.

    20.2. Understand DIR and STC Customer business, service levels, and its customers and respond appropriately.

    20.3. Understand DIR's and STC Customers' technology and sourcing arrangements.

20.4. Use recognized customer service and interpersonal skills, such as telephony skills, communication skills, active listening and customer care training.

20.5. Make appropriate decisions and initiate actions that reflect DIR and STC Customer priorities.

20.6. Understand changes in products and services, as they become part of Service Provider responsibilities.

21. Provision Service Desk Support on a 24 x 7 basis.
22. Provide a single, toll-free (in-country) telephone number for external calls to the Service Desk from Authorized Users where required.
23. Provide DIR and STC Customers with an alternative local number (in-country) for calls to the Service Desk.
24. Identify potential Authorized Users' training requirements, and provide recommended training actions to DIR.
25. Provide and maintain instructions for Authorized Users to access the Services.

    25.1. The instructions will be made available to Authorized Users via the Portal and other media as requested by DIR.

2.1.2 Incident Management

Service Provider will provide Incident Management Services in the form of Tier 2 Support, and Tier 3 Support. This includes supporting activities associated with restoring normal Application operation and minimizing the adverse impact on business operations of STC Customer so that expected levels of service quality and Availability are maintained or exceeded.

The primary activities of Incident Management include:

a. Incident classification and initial support
b. Incident investigation and diagnosis
c. Incident escalation
d. Incident resolution and recovery
e. Incident ownership, monitoring, tracking, and communication

Service Provider shall provide knowledge capture and transfer regarding Incident resolution procedures to support the objective of increasing the number of Incidents capable of being resolved by Tier1 Support.

Service Provider responsibilities for Incident Management include:

1. Comply with MSI policies and procedures for Incident Management.
2. Coordinate with the MSI to develop and approve Service Provider related Incident Management content in the MSI managed Service Management Manual.
3. Utilize the Incident Management System provided by the MSI, for all information related to an incident.
4. 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.
5. Resolve Incidents in accordance with the Service Management Manual, knowledge database documents, and configuration database(s).
6. Identify and classify Incident Priority and handle according to agreed-upon Incident response procedures and assume end-to-end responsibility.
7. Escalate Incidents in accordance with the Service Management Manual, knowledge database documents, and configuration database(s).

8. Provide Tier 2 Support and Tier 3 Support for all supported Applications, unless Tier 3 Support is provided by a third-party supplier.
9. Participate in Incident review sessions
10. Update the progress of an Incident's resolution within the MSI tracking systems through to final closure.
11. Verify that all records (e.g., inventory, asset and configuration management records) are updated to reflect completed / resolved Incidents.
12. Document solutions to resolved Incidents in MSI managed central knowledge base. Accurately update all information pertinent to trouble ticket including general verbiage, codes, etc.
13. Determine wherever possible whether an Incident should initiate a Problem investigation (e.g., whether preventive action may be necessary to avoid Incident recurrence) and, in conjunction with the appropriate Support Tier, raise a Problem record to initiate action.
14. Conduct follow-up with Customer Representative who reported the Incident to verify that the Incident was resolved to their satisfaction.
15. 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.
16. The Service Provider will 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 and will track Software and Equipment to enable the automation of monitoring, detection, and the Resolution of Incidents associated with the Services.
17. Where an OLA does not exist, proactively work with the Service Provider, DIR, and/or DCS Service Providers to deliver the Services required.

2.1.3 Problem Management

Service Provider shall provide Problem Management Services in coordination with the MSI Problem Management structure in order to minimize the adverse impact of Incidents on Customer's business caused by Problems within the Applications and prevent recurrence of Incidents by determining the Problem causing such Incidents so that Service Provider can initiate actions to improve or correct the situation.

Service Provider shall 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 and provide proactive Problem Management to identify and solve Problems and known errors before Incidents occur in the first place, including performing predictive analysis activities, where practical, to identify potential future Problems, develop recommended mitigation plans, and implement approved corrective mitigation actions and processes. Service Provider will also maintain, update and disseminate information about Problems and the appropriate workarounds and resolutions, so that the number and impact of Incidents occurring within the Applications is reduced over time.

The primary activities of Problem Management include:

a. Problem control
b. Error control
c. Proactive prevention of Problems
d. Identifying trends that could result in Incidents or Problems
e. Performing major Problem reviews
f. Providing Problem Management reporting

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

Service Provider is also responsible for implementing resolutions to Problems through the appropriate control procedures, especially Change management and release management, as well as coordinating Problem Management activities with the various teams within Service Provider, Customer and third-party Service Providers responsible for performing Configuration Management, Availability Management, Application Capacity Management, Service Continuity Management, and Service Level management activities.

Service Provider responsibilities for Problem Management include:

1. Coordinate with the MSI to develop and implement policies for Problem Management and root-cause analysis ("RCA") (e.g., events that trigger an RCA).
2. Comply with MSI policies for Problem Management and root-cause analysis.
3. Participate in Problem Management review meetings.
4. Use and update the DIR Problem Management knowledge database managed by the MSI.
5. Perform Problem Management activities in conformance with defined Change management procedures set forth in the MSI managed Service Management Manual.
6. Coordinate with appropriate Incident Management teams and take ownership of Problem Management activities of all Problems that reside in Service Provider's area of responsibility (e.g., detection, logging, root-cause analysis, etc.).
7. 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.
8. Develop and recommend corrective actions or solutions to address recurring Incidents and Problems or failures, as well as mitigation strategies and actions to take to avert potential Problems identified through trend analysis.
9. 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 STC Customer.
10. Create Request for Change ("RFC") documentation with recommended corrective actions to be taken to resolve a Problem and submit to Change management for review and approval using the MSI provided tool.

2.1.4 Request Management and Fulfillment

Service Provider shall be responsible for the fulfillment of Service Requests in compliance with policies and procedures set forth in the Service Management Manual and Managed by MSI.

The Service Provider's responsibilities for Request Management and Fulfillment include:

1. Actively participate with the MSI to develop and document processes.
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. Actively cooperate in information exchange between and among the Service Provider, the MSI, other DCS Service Provider(s), DIR and STC Customer, and/or Third Party Vendor(s) to improve end-to-end Request Management.
4. Integrate the Service Provider's Request Management process with the MSI's Request Management process and systems, where the processes interact.
5. Facilitate the transparency of Request Management through appropriate processes to provide a complete audit trail for the MSI to meet the legislative and policy requirements to which DIR and STC Customer must comply.
6. Actively participate in developing and establishing Request for Solution processes and appropriate mechanisms for the fulfillment of complex requests, requiring design, price, solution and proposals; including appropriate communications to adequately set expectations and promote good customer service.
7. Establish and continually maintain definitions of all services; including descriptions, what services will be standardized, what services require custom solutions, and what services and components can be requested through each medium (e.g. Service Desk, Portal, Service Catalog, Request for Service).

8. The Service Provider will utilize the Request Management System provided by MSI to help provide a level of sophistication to Service Management and overall promote the timely fulfillment of Requests associated with the Services within designated timeframes that accurately prioritizes and coordinates fulfillment efforts according to the business need of DIR and STC Customers, and generally promotes good customer service and expectation setting.
9. Update required information on Service Requests within designated timeframes to support an up-to-date accurate view and reports of Service Requests.
10. Develop formal Service Request closure documentation (package) including completed / approved testing sign-off, and technical documentation and training materials, sign-off of training completion and verification of Application modification / implementation into the production environment

2.1.5 Configuration Management

Configuration management Services are the activities associated with providing a logical model of the Application Maintenance Services by identifying, controlling, maintaining and verifying installed Applications. Service Provider shall account for all Application configurations, provide accurate information on configurations and provide a sound basis for Problem, Change and release management and to verify configuration records against the infrastructure and correct any exceptions within the development environment.

Service Provider shall follow branching scheme and configuration management best practices as outlined by the STC Customer with respect to the development environment. Service Provider will fully support resolution of any code build or merging related issues. If STC Customer has any questions regarding code or data, Service Provider shall answer such questions.

Service Provider also shall cooperate with STC Customer in connection with any audits related to any configuration items identified by STC Customer.

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

1. Develop and document in the MSI Service Management Manual an initial draft of configuration management procedures that meet requirements and adhere to policies defined by STC Customer, maintain such procedures, and recommend refinements of such procedures to Customer and MSI.
2. Work with the MSI to define configuration of the CMDB and required fields and processes etc.
3. Gather requirements from the Customer for CMDB configurations supporting Services.
4. Provide CMDB information to the MSI.
5. Establish and use process interfaces to update CMDB based on changes that occur due to Incident Management, Problem Management, Change management, technical support, maintenance and asset management processes.
6. Establish guidelines for physical and logical separation between development environments in coordination with the STC Customer.
7. Establish the process for deploying and back-out of configuration items in coordination with the STC Customer.
8. Establish configuration baselines as reference points for rebuilds, and provide ability to revert to stable configuration states in coordination with the STC Customer.
9. Integrate the Service Provider's Configuration Management process with the MSI's Configuration Management process and systems, where the processes interact; including providing Configuration data electronically to CMDB provided by MSI.
10. Provide necessary input to the MSI to establish process for verifying the accuracy of configuration items, adherence to configuration management process, and identifying process deficiencies.

2.1.6 Change Management

Service Provider shall perform Change Management Services activities utilizing standardized methods and procedures to provide efficient and prompt handling of all Changes, in order to minimize the impact of Change upon Service quality and consequently to improve the day-to-day operations of the STC Customer. Change management covers all aspects of managing the introduction and implementation of all Changes and in any of the management processes, tools, and methodologies designed and utilized to support the AMS Services.

Service Provider shall assist STC Customer in creating the schedule for any Changes, building and testing such Changes, and producing release notes for such Changes. In addition, Service Provider shall answer questions from STC Customer's development, test and production personnel.

The Change Management process includes the following process steps:

a. Request for Change (RFC) process
b. Recording/tracking process
c. Prioritization process
d. Responsibility assignment process
e. Impact/risk assessment process
f. Establish and manage the schedule of approved Changes
g. Determine metrics for measuring effectiveness of a Change
h. Review / approval process
i. Implementation process
j. Verification (test) process
k. Closure process
l. Coordination of the Change Advisory Board (CAB).

The following list further identifies the Change Management Services that Service Provider will perform.

1. Assist Customer and MSI to refine and improve upon Change Management policies, procedures, processes and training requirements per the Change management process components outlined above, including CAB composition, activities, and the financial, technical, and business approval authorities appropriate to STC Customer requirements.
2. Comply with MSI Change Management policies, procedures, processes and training requirements.
3. Review and approve refinements to Change Management policies, procedures, processes and training requirements.
4. Provide necessary information to STC Customer and MSI to assist in documenting all RFCs, which could include Change cost, risk impact assessment, and system(s) security considerations.
5. Coordinate with Customer to assist in the development of a schedule of planned approved Changes (the "Forward Schedule of Changes" or "FSC").
6. Perform maintenance during regular Maintenance Periods as defined in the Service Management Manual, or as scheduled in advance with the approval of DIR.
7. Provide input to Change logistics.
8. Provide Change documentation as required, to the MSI, including proposed metrics as to how effectiveness of the Change might be measured.
9. As requested participate in CAB meetings to review planned Changes and results of Changes made.
10. Utilize the Change Management System, tools and processes of the MSI for the efficient and effective handling of all Changes (an overall Change Management process), including the Change Advisory Boards (CAB) to manage Changes to the Services, subject to approval from DIR, in a way that minimizes risk exposure and maximizes availability of the Services.

2.1.7 Release Management

Release management is concerned with Changes introduced via the Services and covers both software and the hardware. Release management Services are activities that take a holistic view of a Change so that all of the technical and non-technical aspects of a release related to software, hardware, and network Changes are accounted for and accomplished. These Changes can be implemented by rolling out a combination of new applications or infrastructure software and/or upgraded or new hardware, or simply by making Changes to the service hours or support arrangements.

Release management includes the following processes and activities:

a. Establishing standardized release management policies and procedures
b. Managing release planning and scheduling for overall release schedule, as well as individual releases
c. Establishing and managing a release documentation and identification schema
d. Managing the release design, build, and configuration processes
e. Release testing and testing management
f. Rollout planning including quality plans and back-out plans
g. Release communication, preparation, and training
h. Managing the successful rollout/distribution and installation of all elements of a release
i. Installing only correct, authorized, and tested versions with Changes that are traceable and secure
j. Documenting each release and updating the configuration management database.

Releases consist of a number of Problem fixes and Enhancements to an existing Application. A Release consists of the new or changed software required and any new or changed hardware needed to implement the approved Changes. Releases are generally divided into:

- *Major software releases*, normally containing large areas of new functionality. A major upgrade or release usually supersedes all preceding minor upgrades, releases and emergency fixes.
- *Minor software releases*, normally containing small Enhancements and fixes, some of which may have already been issued as emergency fixes. A minor upgrade or release usually supersedes all preceding emergency fixes.
- *Emergency software*, normally containing the corrections to a small number of known Problems.

The following list identifies the Release Management Services that Service Provider will perform within the development environment.

1. Recommend refinements to the STC Customer and MSI, to Release Management policies, procedures, processes, and training requirements per the release management process components outlined above.
2. Review and approve refinements to Release Management policies, procedures, processes and training requirements.
3. Comply with MSI Release Management policies, procedures, processes, and training requirements.
4. For the development environment support and maintain an appropriate secure environment(s) for all authorized versions of all Applications and Service Provider-Provided Software, in physical or electronic form as applicable (the "Definitive Software Library" or "DSL").
5. Maintain master copies of all new versions of Applications in the secured DSL and update configuration database(s).
6. Provide necessary inputs to STC Customer and MSI to establish, manage, update, and maintain the overall build / release plan and schedule.
7. Establish and administer the version control schema as it relates to release management of Applications other than COTS.
8. Provide regular & timely input to STC Customer to develop, manage, update and maintain release plans for each release in coordination with Change management.
9. Develop quality plans and back-out plans as appropriate for each release with STC Customer.
10. Participate and provide all essential and necessary input for STC Customer audit.

11. Identify and document all configurable items that need to be included in the release, as well as all system inter-dependencies.
12. Assist in the planning and help coordinate the testing process for each release.

    Provide release documentation as required.
13. Implement release in compliance with Change management requirements and adherence to detailed release plans.
14. Provide input and recommendations to help MSI to modify configuration database, asset management items, and service catalog (if applicable) to reflect Changes to configurable items due to the release.

2.1.8 Production Deployment Support

STC Customer routinely schedules production release activities, where the production environment is brought up or down, for example in connection with weekly production releases. Service Provider shall be required to perform testing to determine whether Applications are functioning as expected. Service Provider will support production deployment and perform a check on the Applications in production (check log-files, confirm processes are up, etc.) based upon STC Customer's request. This will be required on a case-by-case basis as requested by STC Customer.

Service Provider development team will be responsible to support STC Customer so that a complete and error free build is configured for release to the production environment. This includes providing release notes per the Service Management Manual.

2.1.9 Service Continuity Management

Service Provider shall support STC Customer in planning service continuity by helping identify potential areas of risk (threats, vulnerabilities), and by suggesting mitigation strategies and recovery approaches. Service Provider is also required to review and validate STC Customer's Service continuity goals and meet any applicable Service Levels.

Service continuity management Services are the activities associated with providing prioritized service continuity and disaster recovery Services for the Applications, and their associated infrastructure. Applications and associated infrastructure will receive disaster recovery Services according to STC Customer's requirements and policies. Service Provider must demonstrate that for Application Services components under its control Service Provider will consistently meet or exceed DIR service continuity and disaster recovery requirements.

The following further identifies the service continuity and disaster recovery Services that Service Provider will perform.

1. Recommend best practices for service continuity and disaster recovery Services strategies, policies and procedures to STC Customer and MSI.
2. Document service continuity and disaster recovery Services procedures that adhere to STC Customer requirements and policies and that are mutually agreed between the STC Customer and Service Provider.
3. Provide disaster recovery Services procedures to STC Customer and MSI.
4. As needed, assist STC Customer in other continuity and emergency management activities.
5. For STC Customer Site(s) and infrastructure develop and maintain a detailed disaster recovery plan to meet service continuity and disaster recovery requirements. Plan shall include plans for data, backups, storage management and contingency operations that provide for recovering STC Customer's systems within established recovery requirement time frames after a disaster affects STC Customer's use of the Services.
6. Establish processes for Service Provider Site(s) and infrastructure to keep disaster recovery plans up to date and reflecting Changes in STC Customer environment.
7. For Service Provider Site(s) and infrastructure perform scheduled disaster recovery tests per STC Customer policies.

8. Track and report disaster recovery test results for Service Provider Site(s) and infrastructure to STC Customer and MSI.
9. Develop action plan to address disaster recovery testing results for Service Provider Site(s) and infrastructure.
10. Implement action plan and provide ongoing status until completion.
11. Initiate disaster recovery Services in the event of a Service Provider disaster recovery situation and notify STC Customer per disaster recovery policies and procedures.
12. Coordinate with STC Customer during a Service Provider disaster recovery situation per disaster recovery policies and procedures.
13. Participate in post-disaster meetings with STC Customer and MSI.

2.1.10 Crisis Management

Crisis management may be necessary depending on the type of business or geographic location where Services are being performed (for example, hurricanes, tornados, riots, terrorist threats). The following further identifies the crisis management Services that Service Provider will perform.

1. Following DIR and STC 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.
2. Following statewide notification pyramid alert support as documented in the applicable business continuity plan.
3. Coordinate with MSI, DIR and STC Customers requirements for Applications / Services that are critical to designated STC Customer emergency management responsibilities such as: Expanded availability windows; Quicker incident response (including break/fix Services).
4. Coordinating with the MSI, DIR and STC Customer regarding variances in Services and potential incremental costs as a result of Crisis Management in compliance with all Service Management Manual procedures.

2.1.11 IT Security Management

Service Provider shall conform to STC Customer security guidelines, including the procedures in Attachment A-4 - Policies, Procedures and Standards, that are in the Service Management Manual so that the security goals are met and all Service Provider Personnel are aware of the risks associated with breaches of security standards. Service Provider will also cooperate with STC Customer in connection with any security audits by sharing requested information and providing access to technical infrastructure.

The following list further identifies the security management Services that Service Provider will perform.

1. Assist in developing security standards, policies and procedures including industry best practices with DCS Customer and MSI.
2. Adhere to the Service Management Manual security requirements, standards, procedures and policies including regulatory requirements.
3. Recommend security improvements based upon current security trends, threats, common exploits, prior experiences, and best practices.
4. Provide a security assessment group to conduct assessments, per an identified schedule, in accordance with STC Customer and Service Provider security policies.
5. Provide security plan based on security requirements, standards, procedures, policies, STC Customer federal, state, and local requirements and risks.
6. Report security violations to STC Customer per STC Customer policies.

7. Review all security patches relevant to STC Customer's environment and classify the need and speed in which the security patches should be installed as defined by security policies.
8. If applicable, in the development environment and as approved by STC Customer, install security patches per Change management process and procedures at Service Provider Site(s).
9. Maintain all documentation required for security assessments, audits and internal control and control testing in the STC Customer repository.
10. Place and support systems with particularly sensitive data in controlled access areas.
11. Limit access to data to authorized Service Provider personnel only.
12. Allow and cooperate with third-party security audits.
13. Participate in STC Customer (MSI) security training.
14. Implement a security awareness program that supports Project Services.
15. As requested, attend Security Management and Risk Management meetings.
16. All Service Provider personnel must have received a CJIS-compliant security Clearance, in accordance with the Agreement and the Service Management Manual.
17. Implement processes and procedures for tracking Clearances for all Service Provider personnel and Third Party Vendors utilizing the comprehensive database for tracking security Clearances provided by the MSI.

2.1.12 Monitoring, Reporting and Review Services

Service Provider shall provide the monitoring, reporting and review Services in accordance with STC Customer's requirements, which include activities associated with: ongoing health checks, quality assurance, quality control, progress monitoring, Service Level reports, code reviews, SDLC-related document reviews, status reports, Problem Management-related reports (i.e., ongoing tracking, analysis, resolution and prevention of Problems), in each case, as related to the MAS Services. The reports to be provided by Service Provider will include all reports in the **Attachment 13-A** (Reports).

The following further identifies the monitoring, reporting and review Services that Service Provider will perform.

1. Provide, maintain and update plans for the Project Services, identifying critical path dependencies
2. Provide weekly status reviews and progress reports for all Project Services via the MSI managed project management tool.
3. Provide monthly service-level performance data against each Service Level requirement, via the MSI managed management tool.
4. Provide milestone achievement data in the MSI managed project management tool.
5. Provide an electronic copy of an applications inventory being maintained.
6. Provide mutually agreed to reports to enable invoice reconciliation.
7. Provide mutually agreed to reports that capture Service Requests demands and measure of ability to satisfy demand to the MSI.
8. Provide mutually agreed reports that represent general health of environments (e.g., changes) as well as reports that represent demand fulfillment in STC Customer terms (e.g., defect corrections/Change requests that have slipped against commitment, backlogged defects/Change requests, Service Requests).
9. Develop improvement plans for services that do not meet Service Level requirements.
10. Provide Service Request response time management reports (including a trend line) for new development work that reflects time to provide time and cost estimates to the MSI.

2.1.13 Availability Management

The activities of the Availability management process include:

a. Analysis of application portfolio management, incidents and capacity to inform Availability requirements
b. Determining business unit Availability Requirements for a new or enhanced Service and formulating the Availability and recovery design criteria for the existing application services so that such Services are designed to deliver the appropriate levels of Availability
c. Determining the critical business functions and impact arising from IT component failure. Where appropriate, reviewing the Availability design criteria to provide additional resilience to prevent or minimize impact to STC Customer's business.
d. Identifying opportunities to optimize the Availability of the Applications to deliver cost effective improvements that deliver tangible business benefits
e. Defining the targets for Availability, Reliability and Maintainability for the IT software components that underpin the application services to enable these to be documented and agreed within Service Levels, and contracts
f. Establishing measures and reporting of Availability, Reliability, and Maintainability, that reflects the STC Customer's business and IT support organization perspectives
g. Monitoring and trend analysis of the Availability, Reliability and Maintainability of IT systems and components
h. Reviewing the application services, system, and component Availability, identifying unacceptable levels, and taking appropriate corrective actions to address Availability shortfalls
i. Investigating the underlying reasons for unacceptable Availability
j. Producing and maintaining a forward-looking Availability plan, which prioritizes and plans overall Availability improvements aimed at improving the overall Availability of the Project Services and Application components so that existing and future business Availability requirements can be met
k. Providing a range of IT Availability reporting to the MSI so that agreed levels of Availability, Reliability and Maintainability are measured and monitored on an ongoing basis

The following list identifies the Availability Management Services that Service Provider will perform.

1. Recommend Availability management policies and procedures and appropriate Availability management tools and methods that support STC Customer's Availability management support requirements.
2. Assist with the implementation of agreed-upon Availability management policies and procedures.
3. Adhere to Availability management policies and procedures.
4. Provide STC Customer-authorized staff, MSI and designated personnel unrestricted read access to all current and historical Availability knowledge base records.
5. Participate in requirements analysis when new IT systems and services are being defined to ensure that Project Services are designed to deliver the required availability levels.
6. Assist in the creation of Availability and recovery design criteria to be applied to new or enhanced Applications and system design.
7. Coordinate with the STC Customer IT service support and service delivery management personnel to research, review, and assess Availability issues and optimization opportunities.
8. Recommend appropriate tools and practices to measure and report on agreed-upon Availability Service Levels for new and enhanced Applications.
9. Assist MSI with the implementation of approved Availability Service Level measurement tools and practices.
10. Monitor and maintain an awareness of technology advancements and IT best practices related to Availability optimization and periodically provide updates to STC Customer.
11. Assist in the coordination of Availability management across all IT service areas with STC Customer and third parties (e.g., public carriers, Internet Service Providers, Infrastructure Service Providers, etc.).

12. Assist STC Customer in Availability assessment review sessions and provide cost-justified improvement recommendations.
13. Coordinate with STC Customer and third-party Service Providers to gather information on IT systems and service Availability issues and trends to be used for trend analysis.
14. Review Full-Service Applications and Interfaces against Availability measures and take appropriate corrective actions to address Availability shortfalls, if such shortfalls are related to such Applications' or Interfaces' code.
15. Provide support and assistance to STC Customer and MSI in investigating the underlying reasons for unacceptable Availability.

2.1.14 Capacity Management

Capacity management Services are the activities associated with matching the evolving demands of STC Customer's business with the capacity of the Applications in a cost-effective and timely manner. The process encompasses the following:

a. Monitoring of performance and throughput of Applications and supporting IT components
b. Understanding current demands and forecasting for future requirements
c. Developing capacity plans which will meet demand and Service Levels
d. Conducting risk assessment of capacity recommendations
e. Identifying financial impacts of capacity plans
f. Undertaking tuning activities

The following list identifies the capacity management Services that Service Provider will perform.

1. Assist in documentation and maintenance of the capacity management procedures in the Service Management Manual
2. Approve capacity management changes to the Service Management Manual
3. Comply with policies and procedures
4. Assist MSI, SCPs, and STC Customers in the capacity management planning process
5. Assess capacity impacts when adding, removing or modifying Applications
6. Assist with capture of trending information and forecasting of future STC Customer capacity requirements based on STC Customer-defined thresholds
7. Recommend Changes to capacity to improve service performance
8. Assess impact/risk and cost of capacity Changes

2.1.15 Technology Refreshment and Replenishment

Technology refreshment and replenishment ("**TR&R**") Services are the activities associated with modernizing the Applications on a continual basis so that the system components stay current with evolving industry-standard technology platforms.

The following list identifies the TR&R Services that Service Provider will perform.

1. As part of its responsibilities, in connection with the Technology Solution Group, recommend TR&R life cycle management policies, procedures and plans appropriate for support of Customer's business requirements.
2. Assist STC Customer and MSI with developing TR&R plans that meet requirements, and adhere to STC Customer policies.
3. Assist STC Customer with the necessary tasks required to implement the TR&R plans.
4. Provide management reports on the progress of the TR&R plans to STC Customer and MSI.

2.1.16 Performance Management

Performance management Services are the activities associated with tuning Managed Application Service components for optimal performance.

The following identifies the performance management Services that Service Provider will perform.

1. Proactively evaluate, identify and recommend configurations or Changes to configurations that will enhance performance.
2. Provide technical advice and support to STC Customer's Application maintenance and development staffs as required.

2.1.17 License Management

License Management Services are the activities associated with tracking and reporting license compliance. The Service Provider is responsible to:

1. Manage STC Customer and Service Provider owned software license inventory using the MSI license management tool.

2.1.18 IT Financial Management

Proper IT Financial Management will provide cost-effective stewardship of the IT assets and the financial resources used in providing IT Services. The Service Provider must provide IT Financial Management Services as described in **Exhibit 4**.

Service Provider responsibilities include:

1. Actively participate with the MSI to develop and document processes.
2. Actively cooperate in information exchange between and among the Service Provider, the MSI, other STC Service Provider(s), DIR and STC Customer, and/or Third Party Vendor(s) to improve end-to-end IT Financial Management.
3. Facilitate the transparency of IT Financial Management through appropriate processes to provide a complete audit trail for the MSI to meet the legislative and policy requirements to which DIR and STC Customer must comply.
4. Integrate Service Provider IT Financial Management process with the MSI's IT Financial Management process, where the processes interact.
5. Integrate Service Provider IT Financial Management process with the other service management processes, especially Service Level Management, Capacity Management, and Configuration Management, as well as areas of governance as described in **Exhibit 6**.
6. Actively support the MSI to assure the proper application of IT Financial Management across all functions and organizations that provide services to STC Customers.
7. Actively participate in regularly scheduled IT Financial Management meetings, included those associated with the requirements for governance as described in **Exhibit 6**.
8. Communicate and coordinate the IT Financial Management processes and policies within Service Provider own organization, and as appropriate to STC Service Providers associated with Services.
9. Actively participate in defining IT Financial Management Policies and procedures, as approved by DIR, which the objectives, scope and principals that will ensure the success of the IT Financial Management processes.

9.1. Provide effective and agreed mechanisms for properly complying with the IT Financial Management policies and procedures.

2.1.18.1 Chargeback and Utilization Tracking System

Service Provider responsibilities include:

1. Utilize the Chargeback and Utilization Tracking System (Chargeback 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.
2. Integrate the Chargeback System with other systems for Service Management, including but not limited to Service Level Management, Capacity Management (CMIS), and Configuration Management (CMS / CMDB).
3. Integrate the MSI Chargeback System with Service Provider's other systems; including all appropriate and required licenses and/or interfaces.
   3.1. Where Service Provider has an internal IT Financial Management System provide for Integration of that system with the MSI Chargeback System, as required by DIR.
   3.2. Provide customization of the integration, as required, to enable IT Financial Management, provide the Services, and meet Service Levels.
4. Provide sufficient detail to support DIR and STC Customers State and Federal funding accounting, grant and audit requirements.
5. Collect and aggregate billing, service provisioning, and service metric information from Service Provider Services
6. Identify unique STC Customer account identifiers to identify Applications and other services information.

2.1.18.2 Chargeback and Utilization Reporting

Service Provider responsibilities include:

1. Support all charges with detailed invoice reports in **Attachment 4-F** and supporting utilization data as described in **Attachment 13-A** at the STC Customer, Resource Units, cost category (e.g. Programs, Divisions, Organization Units) and Resource Unit unique ID level, as required.
2. STC Customers will identify unique Resource Unit IDs and provide cost category mapping through the self- service Portal.
3. Chargeback Service Provider billing will apply all portal changes to accounting information during the invoice period.

2.1.18.3 Chargeback Invoice Consolidation

Service Provider responsibilities include:

1. Provide the MSI with a single monthly Enterprise invoice for Service Provider Services and designated Third Party Vendors.
2. Provide the MSI a single monthly chargeback invoice for each STC Customer for Service Provider Services and designated Third Party Vendors.

2.1.18.4 Invoice Dispute Processing

Service Provider responsibilities include:

1. Actively participate in developing and maintaining the processes for the resolution of invoice disputes within designated timeframes.
2. Provide effective and agreed mechanisms for crediting DIR and STC Customers as appropriate.
3. Effectively execute the processes to record, track and manage incidents of invoice disputes.
4. Research and review invoice disputes for completeness and supporting data accuracy and, when necessary, request clarifying data from DIR or STC Customer.
5. Support and initiate additional treatment of invoice disputes to facilitate resolution within designated timeframes.
6. Ensure that incidents of invoice disputes are continually updated, at a minimum on a weekly basis.
7. Keep the MSI informed of activity and anticipated Resolution times for active incidents of invoice disputes.
8. Allow DIR to monitor and validate invoice dispute process on an ongoing basis.
9. Provide a process for escalating to Service Provider management incidents of invoice disputes not Resolved within the time frames established within DIR policies.

2.2 Reports

Service Provider shall provide the reports via the MSI managed Portal as specified in **Attachment 13-A**.

2.3 Assumptions, Dependencies and Constraints

Assumptions, Dependencies and Constraints will be defined if the Service Provider is engaged by a STC Customer to propose or deliver services.