SCHEDULE 2A

IT SERVICE MANAGEMENT AND LIFE CYCLE SERVICES SOW

Table of Contents

List of Tables

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

i

This is Schedule 2A (IT Service Management and Life Cycle Services SOW) to the Agreement between the City of San Diego ("Client" or "the Client") and Vendor ("Vendor"). Unless otherwise expressly defined herein, the capitalized terms used herein shall have the meaning assigned to them in Attachment A (SOW Definitions).
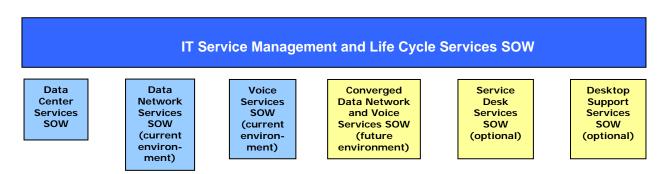
1.0 IT Service Management and Life Cycle Services Overview and Objectives

1.1 IT Service Management and Life Cycle Services Overview

This Schedule 2A (IT Service Management and Life Cycle Services SOW) is the Statement of Work (or "SOW") that sets forth the roles and responsibilities of Parties for the set of common services that apply to the provision, delivery, and management of all IT Services within the scope of this Agreement. Vendor shall provide these services across all Service Areas defined herein and all future IT Service Areas that are added to this Agreement.

As depicted in Figure 1 below, Services, activities and roles and responsibilities described in this SOW are within the scope of each SOW for the Service Areas and shall be included within the Fees for each Service Area specified in Schedule 3 (Fees) to the Agreement. Figure 1 depicts the relationship between the IT Service Management and Life Cycle Services SOW, and all SOWs within the scope of the Agreement.

Figure 1: **SOW Service Areas**

1.1.1 Service Area Maintenance and Changes

In order to perform regular maintenance and planned system changes, a weekly Maintenance Window is scheduled from

- 6:00 p.m. Pacific Time (PT) on Wednesday until 6:00 a.m. PT on Thursday for all Applications

- 4:00 a.m. PT – 4:00 p.m. PT on the second Sunday of the month for network infrastructure services

- 4:00 a.m. PT – 4:00 p.m. PT on the fourth Sunday for non-network infrastructure (e.g., database updates, server updates, etc.)

All maintenance performed during these hours shall be approved by a Change Control Board. Actual duration of changes must be specified in an approved change request and are usually for

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

1

shorter time periods within the specified Maintenance Windows. Some test system changes and most production changes that require downtime or have significant risk are scheduled during the weekly Maintenance Window. It is a requirement therefore that Vendor and Client responsible groups be available weekends and nights as required to complete changes and requests in a timely and non-disruptive manner.

Tasks which require system downtime outside of the Maintenance Window, such as during the business day, shall be approved by the Client and shall be scheduled to minimize business impact. Select non-production system changes that require downtime may be scheduled weekdays between 8:00 p.m. PT and 6:00 a.m. PT to minimize impact on development activities.

1.2   Service Objectives

The following are the key high-level Service objectives the Client expects to achieve through this IT Service Management and Life Cycle Services Statement of Work (SOW):

- Ensure that critical IT life cycle and IT Service Management (ITSM) functions are included in all current and future Services Area SOWs

- Receive IT Services that consider an end-to-end enterprise view across all IT Service Areas and across all Third Party providers, vendors, Interfaces, products and solutions and maintain a security posture and security program across all Service Areas

- Receive Services based on current industry standards and practices (applicable industry standards include BSI, ISO, COBIT, ITIL/ITSM)

- Provide a consistent set of IT life cycle services applicable to all current and future Software, hardware and services introduced to the service environment

- Proactively address the need for replacing obsolete equipment and performing technology refresh

- Continually improve Service delivery while lowering IT cost over time

- Achieve the Service Level Requirements (SLRs) identified in Section 4 below including achieving the required customer satisfaction levels

2.0   IT Service Management and Life Cycle Requirements

Vendor is responsible for ensuring that Service Area services, as defined in the SOWs listed below, are integrated and consistent with the IT Service Management and Life Cycle Services defined in this SOW:

- Schedule 2B – Data Center Services SOW

- Schedule 2C – Service Desk Services, per the Service Commencement Date for this tower of service.

- Schedule 2D – Desktop Support Services, per the Service Commencement Date for this tower of service.

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

2

2.1 Service Descriptions and Roles & Responsibilities

Vendor is responsible for ensuring that all Service Area Services are integrated and consistent with this IT Service Management and Life Cycle Services SOW.

2.1.1 General Responsibilities

The following table identifies general roles and responsibilities associated with this SOW. An "X" is placed in the column under the Party that shall be responsible for performing the task. Vendor responsibilities are indicated in the column labeled "Vendor."

Table 1.   General Services Roles and Responsibilities

General Services Roles and Responsibilities	Vendor	Client
1. Provide Services that support Client requirements (e.g., business, technical, End User requirements)	X	
2. Provide Client applicable SOPs		X
3. Comply with Client SOPs (e.g., SOPs for information, information systems, personnel, physical and technical security)	X	
4. Provide Client applicable laws, regulations and Client policies		X
5. Conform to changes in laws, regulations and Client policies. Major changes impacting Services scope shall be addressed through the Service Change process	X	
6. Interface, manage and coordinate, as appropriate, Vendor Subcontractors and other Third Parties (e.g., network circuit provider, Software vendors) in order to meet Service requirements and SLRs	X	
7. Measure and report performance against SLRs	X	
8. Measure and report performance against mutually agreed Key Performance Indicators (KPIs)	X	
9. Provide Vendor with physical access to Client sites that is necessary to perform Services during scheduled hours, and after hours and emergencies as required		X
10. Provide available documentation relative to the Service Area Services as may reasonably be requested by Vendor		X
11. Coordinate all Changes to the Service Areas that may affect the SLRs of any other Service Area or Third Party	X	
12. Provide a single secure web portal for Client access to all account documentation as described in the IT Service Area SOWs (e.g., project plans and schedules, configuration diagrams, management reports, SLR reports, procedures, meeting minutes, change notices)	X	
13. Deliver Services consistent with current (as released within the last 12 months) BSI 15000, ISO 9000, ISO 17799, ISO 20000, ISO 27001, COBIT, and ITIL/ITSM standards as applicable to each Service Area	X	

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

3

General Services Roles and Responsibilities	Vendor	Client
14. Provide Vendor with facilities for Vendor's on-site personnel, as required to deliver the Services		X
15. Support Client internal and Third Party financial and technical assessment activities conducted in the Client environment (e.g., internal and external audits)	X	
16. Recommend Vendor standard procedures for each of the Services/sub-services areas defined in this SOW and all Service Area SOWs to which this SOW is applicable	X	
17. Develop, document and maintain in the Policies, Standards and Procedures Manual operational procedures for each of the Services/sub-services areas defined in this SOW and all Service Area SOWs to which this SOW is applicable	X	
18. Review, provide additional procedures as required and approve operational procedures for each of the Services/sub-services areas defined in this SOW and all Service Area SOWs to which this SOW is applicable		X

2.1.2 Project Management Services

Vendor shall provide Project Management Services required to manage Vendor services, activities and tasks associated with vendor managed work. The following table identifies the Project Management Services roles and responsibilities that Vendor and Client shall perform.

Table 2.   Project Management Services Roles and Responsibilities

Project Management Services Roles and Responsibilities	Vendor	Client
Project Oversight		
1. Plan, monitor, and manage project-related work provided by Vendor	X	
2. Create, maintain and provide all appropriate project plans, project time and cost estimates, technical specifications, management documentation and management reporting for Vendor activities, in a mutually agreed to format.	X	
3. Participate in meetings to review technology or business plans, and recommend appropriate IT services and projects in support of such plans	X	
4. Maintain appropriate levels of industry knowledge in the Client's business to provide support and recommendation of projects	X	
5. Maintain and update a list of the Vendor managed projects, work activities, and prioritization of projects	X	
6. Participate in relevant project governance meetings	X	
Project Initiation		
7. Provide user requirements, specifications, high level schedule, and prioritization for Client-sponsored projects		X

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

4

Project Management Services Roles and Responsibilities	Vendor	Client
8. Prepare proposals and project plans as requested by the Client or as appropriate. Such proposals and plans shall include the following based on whether the project is related to in-scope base services or an out of scope project: • Deliverable(s) to be provided • Technical approach and solution • Description of any equipment, Software, or other materials required for the project and ongoing support • Expected project schedule and any time constraints or material assumptions • Total cost of the project (including fees paid to Vendor as well as any retained expenses), and whether the cost is included in the Baseline Fees • Ongoing annual cost of the project post-implementation (including fees paid to Vendor as well as any retained expenses), and whether the cost is included in the Baseline Fees • Other material assumptions, including any support required from Client or its Third Parties • Provide service amendment as appropriate	X	
9. Review and approve project proposals and plans		X
Project Support		
10. Conform as feasible, to the Client's established IT lifecycle (ITLC) methodology to plan, initiate, control, and implement projects	X	
11. Manage Vendor tasks and resources associated with the project, and coordinate activities with the Client	X	
12. Make any changes related to the project in accordance with approved change management procedures and gain required approvals	X	
13. Identify scope changes and propose alternatives and, if necessary, provide appropriate change documentation	X	
14. Approve project changes to scope, schedule, pricing, services, or Deliverables		X
15. Use applicable project management tools and methodologies, which employ a regular reporting mechanism to identify tasks, develop and present status reports, and identify potential risks and problems	X	
16. Communicate project status as part of standard project management meetings, or other such meetings as agreed, with the Client	X	
17. Develop, maintain, and update project schedules by Deliverable	X	

Project Management Services Roles and Responsibilities	Vendor	Client
18. Monitor and report progress, providing corrective actions against the plan for each project, if needed	X	
19. Monitor, track, and report actual results versus forecasted results per project Deliverable	X	
20. Identify, log, and follow defined processes for risk and issue mitigation	X	
21. Identify, log, and follow defined processes for scope change management	X	
22. Conduct or support project closeout to include project estimated cost, actual cost, and key knowledge acquired for Vendor project responsibilities	X	
23. Support and create as required project documentation and submit to the Client's electronic document management system or such other system agreed to by both Parties	X	
24. Review and approve Project Management Services related Deliverables		X

2.1.3   IT Lifecycle & Operations Services

The IT Lifecycle (ITLC) and Operations Services described in the following sub-sections shall apply to current and future Client Service Area environments (e.g., Software, hardware, Services). Vendor shall manage all Service Area IT lifecycle activities in accordance with the following common lifecycle and operational services, unless approved by the Client. Vendor shall develop, document and maintain Service Area specific activities and procedures associated with these ITLC and operations services in the Policies, Standards and Procedures Manual.

2.1.3.1   *Planning and Analysis*

Planning and Analysis Services are activities associated with:

- Researching new technical trends, products and services, such as hardware components, System Software, and networks that offer opportunities to improve the efficiency and effectiveness of the Service Areas
- Investigating methods to improve the quality of IT Services (e.g., productivity and operational improvements, defect reduction)
- Planning for the introduction of major Changes, enhancements and new Client Application programs
- Continuously improving the Client technical environment

The following table identifies the Planning and Analysis Services roles and responsibilities that Vendor and Client shall perform.

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

6

Table 3.   Planning and Analysis Services Roles and Responsibilities

Planning and Analysis Services Roles and Responsibilities	Vendor	Client
1. Define Client requirements at the enterprise level for all Service Areas (e.g., business, technology strategy, functional, Availability, capacity, performance, backup and IT continuity Service)		X
2. Perform technical and Service Planning and Analysis Services based on Client requirements (e.g., Availability, capacity, performance, backup and IT Continuity and Disaster Recovery Services)	X	
3. Provide recommendations for new infrastructure and Services based on planning and analysis results	X	
4. Review and approve Planning and Analysis recommendations		X
5. Provide information and data as available for Planning and Analysis Services (e.g., utilization, business capacity reports, roll out plans)		X
6. Continuously monitor technical trends and report quarterly on products and services with potential use for the Client as it aligns with the Client's business and technology strategy	X	
7. Perform semi-annual assessments for the implementation of new technologies that best meet Client requirements and cost objectives		X
8. Conduct semi-annual technical and business planning sessions to establish standards, architecture and project initiatives per the planning and analysis results		X
9. Participate in semi-annual technical and business planning sessions to establish standards, architecture and project initiatives	X	
10. Conduct regular planning and conduct semi-annual planning meeting with the Client for technology refreshes and upgrades	X	
11. Participate in regular planning and semi-annual planning meeting with Vendor for technology refreshes and upgrades		X
12. Conduct semi-annual technical reviews and provide the Client with written recommendations for improvements that increase efficiency and effectiveness or reduce costs per the planning and analysis results	X	
13. Participate in project specific planning sessions and provide proposals with timelines, critical milestones and estimates on timing and costs	X	

2.1.3.2 Requirements Definition

Requirements Definition Services are the activities associated with the assessment and definition of Client information system requirements (e.g., performance, disaster recovery, security requirements) that also comply with regulatory and Client Standard Operating Procedures (SOPs). These requirements drive the technical design and operations for the

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

7

Vendor managed Service Areas. The following table identifies the Requirements Definition Services roles and responsibilities that Vendor and the Client shall perform**.**

Table 4.   Requirements Definition Services Roles and Responsibilities

Requirements Definition Services Roles and Responsibilities	Vendor	Client
1. Define requirements development documentation format and content		X
2. Involve Vendor in Third Party application technical design activities		X
3. Provide appropriate technical support staff (e.g., enterprise architects and engineers) to participate in technical requirements development with application team (e.g., Client, Vendor, Third Party application developers)	X	
4. Conduct interviews, group workshops, and surveys to determine infrastructure requirements (e.g., system Interface, performance, Availability, disaster recovery)		X
5. Participate in requirements gathering activities (e.g., focus groups, interviews)	X	
6. Provide written information in sufficient detail pertaining to the Requirements Definition Services to enable development of appropriate requirements documentation (e.g., business requirements documentation)		X
7. Document requirements required to deliver Services using approved requirements standards (e.g., system specifications, data models, upgrade requirements, conversion requirements, network design schematics)	X	
8. Determine and document required Service Area component upgrade, replacement and/or conversion requirements (e.g., hardware, Software, networks)	X	
9. Ensure requirements meet defined security requirements	X	
10. Document cross Service Area integration requirements	X	
11. Recommend user acceptance test (UAT) criteria		X
12. Participate in defining UAT criteria	X	
13. Review and approve all UAT criteria		X
14. Provide documented requirements and UAT criteria per approved requirements standards		X
15. Review and approve all requirements documents		X
16. Provide infrastructure cost estimates based on requirements for budgeting purposes	X	

2.1.3.3 Design Specifications

Design Specification Services are the activities and Deliverables associated with translating Client developed information system standards and requirements (e.g., architectural, business,

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

8

security, performance, availability, regulatory) into detailed technical designs and specifications for Client review and approval. The following table identifies the Design Specifications Services roles and responsibilities that Vendor and the Client shall perform.

Table 5.   Design Specifications Services Roles and Responsibilities

Design Specification Services Roles and Responsibilities	Vendor	Client
1. Provide Vendor with written information in sufficient detail pertaining to the design specifications to enable creation of the appropriate technical designs		X
2. Conduct site surveys for design efforts as required to deliver design specifications and plans	X	
3. Document and deliver design specifications, including cross Service Area specifications	X	
4. Review and approve design specifications		X
5. Provide infrastructure cost estimates based on design results for budgeting purposes	X	

2.1.3.4 Acquisition Management Services

Acquisition Management Services are the activities associated with the pricing, evaluation (technical and costing), selection and acquisition of new and upgraded Service Area components (e.g., hardware, Software). Acquisition Management Services generally apply to the following Service Areas: Data Network, Voice, and Converged Data Network and Voice; however, Vendor may have some collateral and shared responsibilities under Data Center Services or Service Desk and Desktop Support Services. The following table identifies the Acquisition Management Services roles and responsibilities that Vendor and the Client shall perform.

Table 6.   Acquisition Management Services Roles and Responsibilities

Acquisition Management Services Roles and Responsibilities	Vendor	Client
1. Coordinate temporary storage of ordered Data Center equipment pending scheduling of installation	X	
2. Coordinate delivery and installation of new products and services, as required, related to Data Center Services or data center facilities (including Client facilities where applicable)	X	
3. Review and approve selection of hardware to be installed in Client facilities and Software to be installed on Client hardware		X
4. Review and approve installation Acceptance process		X
5. Adhere to Client installation Acceptance process	X	
6. Terminate, dispose of according to the Client Asset disposal guidelines and relocate Client-owned Assets as needed/specified and provide disposition reports as required by the Client	X	

2.1.3.5 Integration and Testing

Integration and Testing Services are the activities associated with ensuring that all individual Service Area components (e.g., hardware, Software, middleware, Interfaces, network) configured with or added to the environment work together cohesively to achieve the intended results and meet Client requirements. The following table identifies the Integration and Testing Services roles and responsibilities that Vendor and the Client shall perform.

Table 7. Integration and Testing Services Roles and Responsibilities

Integration and Testing Services Roles and Responsibilities	Vendor	Client
1. Conduct testing of infrastructure changes in non-production environments	X	
2. Prepare test plans for any proposed Changes to Service Area components	X	
3. Review and approve test plans for any proposed Changes to Service Area components/configurations		X
4. Conduct integration and security testing (using approved test plans) for all new configurations and upgraded equipment (e.g., hardware, Software, middleware, Interfaces, network) or services to include unit, system, integration and regression testing based on requirements defined in requirements and design documents	X	
5. Evaluate all new and upgraded Service Area components, configurations or services for compliance with Client security policies, regulations and procedures	X	
6. Assess and communicate to the Client the overall impact and potential risk to Service Area components prior to implementing Changes	X	
7. Provide the Client with test results for Changes to Service Area components and configurations	X	
8. Review and approve test results		X
9. Define UAT requirements		X
10. Stage new and upgraded equipment, Software or services to smoothly transition to all existing infrastructure environments based on requirements defined in requirements and design documents	X	
11. Perform modifications and performance enhancement adjustments to System Software and utilities as a result of changes to architectural standards, additions and upgrades to the environment or configuration changes	X	
12. Test new releases of supported hardware and Software to ensure required performance and functionality is maintained and in conformance with SLRs	X	
13. Support middleware required to integrate Software, hardware and Interface with Third Parties	X	

Integration and Testing Services Roles and Responsibilities	Vendor	Client
14. Perform Configuration Management and Change Management activities related to Integration and Testing Services	X	

2.1.3.6 *Implementation and Migration*

Implementation and Migration Services are the activities associated with the installation of new and upgraded IT components (e.g., hardware, Software and network components). The following table identifies the Implementation and Migration Services roles and responsibilities that Vendor and the Client shall perform.

Table 8. **Implementation and Migration Services Roles and Responsibilities**

Implementation and Migration Services Roles and Responsibilities	Vendor	Client
1. Notify Vendor of application, Software and hardware implementation and migration plans		X
2. Coordinate and review all Implementation and migration plans and schedules with the Client in advance, in accordance with Change Management Services policies	X	
3. Approve Implementation and Migration plans and schedules		X
4. Conduct pre-installation site surveys as required to meet implementation requirements	X	
5. Perform engineering functions required to implement design plans for additional or new products and services	X	
6. Develop and deliver engineering plans where there is an impact on Client entities/facilities and/or other Third Party agreements	X	
7. Perform engineering functions required to implement and manage Service Area Services at Client sites	X	
8. Review and approve engineering plans and procedures where there is an impact on other Client entities/facilities/Third Party agreements		X
9. Implement enhancements to technical architecture or Services provided	X	
10. Install new or enhanced Service related components (e.g., hardware, Software, middleware, utilities, networks, peripherals, configurations)	X	
11. Perform Service Area component upgrades as a result of new and enhanced applications, architectures and upgrade plans and requirements (e.g., hardware, Software, middleware, utilities, networks, peripherals, configurations)	X	
12. Coordinate Implementation and Migration Services activities with Client IT staff and service desk	X	
13. Coordinate and support data migration and conversion by electronic or manual methods as a result of implementation or migration (e.g., databases)	X	

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

11

Implementation and Migration Services Roles and Responsibilities	Vendor	Client
14. Perform appropriate tests on all installs, moves, adds, changes and disposals (IMACDs) per requirements	X	
15. Determine UAT requirements		X
16. Conduct and document UAT plans and results per requirements		X
17. Review and approve UAT plans and results		X
18. Maintain test cases/scripts in configuration management database to enable incremental fall back capability per Client policy	X	
19. Provide Client IT technical staff with training related to the implementation of new products and Services per requirements	X	

2.1.3.7 Training and Knowledge Transfer

Training and Knowledge Transfer Services consist of the following two types of training Vendor shall provide:

- Training of Vendor staff for the improvement of skills through education and instruction. In addition, Vendor shall participate in any initial and on-going training required to support the Client's technical environment and that would provide a learning opportunity about the Client's business

- Training/Knowledge Transfer for Client retained technical staff regarding the Vendor managed Client environment (e.g., Vendor Service delivery processes, technical configurations)

The following table identifies the Training and Knowledge Transfer Services roles and responsibilities that Vendor and the Client shall perform.

Table 9. Training and Knowledge Transfer Services Roles and Responsibilities

Training and Knowledge Transfer Services Roles and Responsibilities	Vendor	Client
1. Develop and deliver a training program to instruct Client and authorized entities personnel on the provision of Vendor Services and the Vendor managed Client environment (e.g., "rules of engagement", requesting services)	X	
2. Review and approve Vendor developed training program		X
3. Develop and implement knowledge transfer procedures to ensure that the appropriate number of Vendor staff understands key components of the Client business and technical environment	X	
4. Participate in Client delivered instruction on the Client business and technical environment	X	

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

12

Training and Knowledge Transfer Services Roles and Responsibilities	Vendor	Client
5. Provide support staff that are technically qualified to perform their role	X	
6. Develop technical training materials, training plan, and provide training to Client retained technical staff when substantive (as defined between Client and Vendor) technological Changes (e.g., new systems or functionality) are introduced into the Client environment	X	
7. Provide and maintain training materials for the applicable personnel on Client business and technical environments	X	
8. Review and approve training materials		X

2.1.3.8 Documentation

Documentation Services are the activities associated with developing, revising, maintaining, reproducing, and distributing Service Area information in hard copy and electronic form for each specific SOW. The following table identifies the Documentation Services roles and responsibilities that Vendor and the Client shall perform.

Table 10.   Documentation Services Roles and Responsibilities

Documentation Services Roles and Responsibilities	Vendor	Client
1. Provide output in agreed format for support of activities throughout the life cycle of Services as specified in each Service Area	X	
2. Document system specifications and configurations (e.g., interconnection topology, configurations)	X	
3. Provide Client operating requirements		X
4. Develop, document and maintain Client operating procedures documentation (e.g., boot, failover, spool management, batch processing, backup)	X	
5. Review and approve standard operating procedures documentation		X
6. Document job production and maintenance schedules	X	
7. Review and approve job production and maintenance schedules and documentation		X
8. Provide the Client with a copy of or access to any Vendor or Third Party-supplied documentation (including updates thereto)	X	

2.1.3.9 End User Administration

End User (User ID) Administration Services are the Services and activities associated with managing and coordinating account activation, termination, changes, and expiration, and the management of End User resources. In general, the Client shall retain End User Administration responsibilities (e.g., Active Directory administration). Vendor shall provide User ID administration support while enforcing Client information security application and system access

requirements for all Enterprise applications. The following table identifies the End User Administration roles and responsibilities that Vendor and the Client shall perform.

Table 11.   End User Administration Services Roles and Responsibilities

End User Administration Services Roles and Responsibilities	Vendor	Client
1. Provide End User ID tracking and regulatory compliance requirements and approval policies		X
2. Establish End User ID administrative security procedures and practices to ensure that all End User IDs are authenticated (for example, encryption, minimal level, password) for operating systems and databases (excludes applications)		X
3. Define application level role responsibility		X
4. Maintain a secure environment through appropriate control of user accounts and access privileges	X	
5. Add, change, delete, or revoke End User IDs that access applications controlled by Client, per the established security standards		X
6. Add, change, delete, or revoke End User IDs that access applications that are controlled by Vendor, per the established security standards	X	
7. Perform Password Resets for End Users per the established security guidelines		X
8. Perform Password Resets for End Users per the established Client security guidelines (Service Desk function)	X	
9. Provide remote access administration (e.g., VPN access, SecurID tokens)		X
10. Provide audit trail for all End User ID activities for Client Systems (e.g., creation, modification, and deletion of IDs)	X	
11. Manage and maintain system accounts	X	
12. Approve and audit system accounts that are managed and maintained by the Vendor		X
13. Create End User ID administration processes and SOPs as new applications are introduced into the Client environment		X
14. Create and update End User ID management Software for automated approval workflow as new requirements are defined by the Client		X

2.1.3.10 Break/Fix and Maintenance

Break/Fix and Maintenance Services are the activities associated with the maintenance and repair of in scope hardware, Software and networks to include Break/Fix and Software maintenance (e.g., deploying emergency and standard Software updates, patches, hot packs). In addition, Vendor shall maintain installed Software product version levels at no more than two (2) versions behind the current commercial release, as approved by the Client. The following

table identifies the Break/Fix and Maintenance Services roles and responsibilities that Vendor and the Client shall perform.

Table 12. **Break/Fix and Maintenance Services Roles and Responsibilities**

Break/Fix and Maintenance Services Roles and Responsibilities	Vendor	Client
1. Develop and implement maintenance schedules based on Client approved Maintenance Window	X	
2. Define dispatch requirements and point-of-service locations		X
3. Provide maintenance and Break/Fix support in Client defined locations, including dispatching repair technicians to the point-of-service location if necessary	X	
4. Perform diagnostics and maintenance on Service Area components (e.g., hardware, Software, peripherals, networks, servers and special purpose devices)	X	
5. Install manufacturer field change orders, service packs, firmware, and Software maintenance releases, etc.	X	
6. Perform product patch, "bug fix," service pack installation or upgrades to the current installed version in accordance with ITLC services and Change Management procedures	X	
7. Perform major Software release upgrades	X	
8. Perform maintenance related Software distribution and version control (e.g., Software updates, upgrades, emergency and standard patches) using industry standard automated Software distribution and patch management tools across applicable Vendor supported technology and Service Areas	X	
9. Manage centralized software/image deployment tools (e.g. Altiris, SCCM, SUS). Develop distribution packages to patch and upgrade Microsoft and 3rd party applications distributed in the core image and deployed as departmental applications.	X	
10. Coordinate with Client and Third Parties (e.g., Software vendors/developers, other Client service providers) to develop the Software release matrix	X	
11. Maintain Software release matrices across all supported IT environments (e.g., development, QA, and production environments)	X	
12. Validate and approve the Software release matrix		X
13. Replace defective parts including preventive maintenance, with Client provided parts, according to the manufacturer's recommended maintenance schedule and published mean-time-between failure rates	X	
14. Conduct maintenance and parts management and monitoring during warranty and off-warranty periods	X	

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

15

Break/Fix and Maintenance Services Roles and Responsibilities	Vendor	Client
15. Manage hardware, Software, peripherals, Services and spare parts to meet SLRs, minimize down time and minimize Client resource requirements	X	

2.1.3.11 Backup and Recovery

Backup and Recovery Services are the activities associated with providing ongoing Backup and Recovery capabilities according to Client schedules and requirements for identified Service Area components (e.g., data center servers, network routers, local department servers/server rooms). Vendor must demonstrate that it will consistently meet or exceed Client's ongoing Backup and Recovery requirements. The following table identifies Backup and Recovery Services roles and responsibilities that Vendor and the Client shall perform.

Table 13.   Backup and Recovery Services Roles and Responsibilities

Backup and Recovery Services Roles and Responsibilities	Vendor	Client
1. Manage backup media	X	
2. Develop and maintain backup schedule in accordance with Client requirements	X	
3. Provide recovery and backup requirements including schedules, and any updates thereto for Service Area components		X
4. Perform Service Area component backups and manage to established retention periods	X	
5. Perform encrypted backups where required by the Client	X	
6. Archive data media at a secure offsite location near the disaster recovery site	X	
7. Provide ongoing media testing per SLRs for ability to recover data	X	
8. Ensure ongoing capability to recover archived data from media as specified (i.e., backwards compatibility of newer backup equipment)	X	
9. Test backup media to ensure incremental and full recovery of data is possible and ensure Service Area component integrity, as required or requested by the Client	X	
10. Recover files, file system or other data required from backup media, as required or requested by the Client	X	
11. Provide full backup, files or other data on Client-supplied media (e.g., tape, optical disk) as requested by the Client	X	

2.1.3.12 Technology Refreshment and Replenishment

Technology Refreshment and Replenishment (TR&R) Services are the activities associated with modernizing the IT infrastructure on a continual lifecycle basis to ensure that the system components stay current with evolving industry standard technology platforms. A TR&R schedule and plan for each Service Area shall be developed and maintained by the Vendor in

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

16

Attachment I – Technology Refresh Plan. The following table identifies the Technology Refreshment and Replenishment Services roles and responsibilities that Vendor and the Client shall perform.

Table 14.   Technology Refreshment and Replenishment Services Roles and Responsibilities

TR&R Services Roles and Responsibilities	Vendor	Client
1. Develop, document and maintain TR&R schedules and plans for each Service Area	X	
2. Perform the necessary services and tasks required to fulfill the TR&R plans	X	
3. Provide management reports on the progress of the TR&R plans as defined in Attachment J - Reports	X	
4. Implement TR&R plan and provide status reports regarding TR&R implementation status as required	X	
5. Periodically review and approve the TR&R implementation plans to ensure they properly support Client business requirements		X

2.1.4   Service Delivery

2.1.4.1 Capacity / Availability Management

Capacity / Availability Management Services are the activities associated with ensuring that the capacity and availability of the Data Center infrastructure matches the evolving demands of Client business in the most cost-effective and timely manner. Vendor shall provide comprehensive capacity and availability management for all Service Areas. Capacity and availability management will mitigate service degradation and Outages due to increases in utilization of Services and infrastructure. Additionally, it will be used to support proactive development, maintenance, and communication of tactical and strategic technology plans, and to accommodate Client growth or changing business requirements.

The following table identifies the Capacity / Availability Management Services roles and responsibilities that Vendor and the Client shall perform.

Table 15.   Capacity / Availability Management Services Roles and Responsibilities

Capacity / Availability Management Services Roles and Responsibilities	Vendor	Client
1. Establish a comprehensive Capacity / Availability Management planning process	X	
2. Review and approve Capacity / Availability Management planning process		X
3. Define, provide and implement automated and manual tools that allow for the effective capacity / availability monitoring/trending and reporting of IT infrastructure, applications and IT components	X	
4. Develop capacity / availability plans that meet Client demand and SLRs	X	

Capacity / Availability Management Services Roles and Responsibilities	Vendor	Client
5. Review and approve capacity / availability plans		X
6. Identify future business requirements that will alter capacity / availability requirements (e.g., strategic and operational plan, demand management plan)		X
7. Define future capacity / availability requirements and define thresholds		X
8. Participate in all capacity / availability planning reviews		X
9. Assess capacity / availability impacts to all technology when adding, removing or modifying Services, applications and infrastructure	X	
10. Continually monitor IT resource usage to enable proactive identification of capacity / availability issues	X	
11. Capture capacity availability trending information and forecast future Client capacity / availability requirements based on Client defined thresholds	X	
12. Assess Incidents/Problems related to throughput performance	X	
13. Recommend changes to capacity to improve service performance and/or reduce costs	X	
14. Assess impact/risk and cost of capacity changes	X	
15. Approve capacity / availability related recommendations and implementation plans		X
16. Maintain capacity levels to optimize use of existing IT resources and minimize Client costs to deliver Services at agreed to SLRs	X	
17. Ensure adequate capacity / availability exists within the IT environment to meet SLRs taking into account daily, weekly, hardware and Software lifecycle and cyclical business variations in capacity demands	X	
18. Provide Asset utilization reporting	X	

2.1.4.2 Performance Management

Performance Management Services are the activities associated with tuning Service Area components within and across all Service Areas for optimal performance. The following table identifies the Performance Management Services roles and responsibilities that Vendor and the Client shall perform.

Table 16.   Performance Management Services Roles and Responsibilities

Performance Management Services Roles and Responsibilities	Vendor	Client
1. Perform Service Area component tuning to maintain optimum performance in accordance with Change Management procedures	X	

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

18

Performance Management Services Roles and Responsibilities	Vendor	Client
2. Manage Service Area component resources to meet defined Availability and performance SLRs	X	
3. Provide regular monitoring and reporting of Service Area component performance, utilization and efficiency	X	
4. Proactively evaluate, identify and recommend configurations or changes to configurations that will enhance performance	X	
5. Develop and deliver improvement plans as required to meet SLRs	X	
6. Review and approve improvement plans		X
7. Implement improvement plans and coordinate with Third Parties as required	X	
8. Provide technical advice to support Client internal and Third Party technology maintenance and development staffs as required	X	

2.1.4.3 Service Level Monitoring and Reporting

Service Level Monitoring and Reporting Services are the activities associated with the monitoring and reporting of Service delivery with respect to SLRs. In addition, Vendor shall report system management information (e.g., performance metrics, and system accounting information) to the designated Client representatives in a format agreed to by the Client. The following table identifies the Service Level Monitoring and Reporting Services roles and responsibilities that Vendor and the Client shall perform.

Table 17.   Service Level Monitoring and Reporting Services Roles & Responsibilities

Service Level Monitoring and Reporting Services Roles and Responsibilities	Vendor	Client
1. Define Service Level Monitoring and Reporting Services requirements and policies		X
2. Define SLRs		X
3. Report on SLR performance and improvement results	X	
4. Coordinate SLR monitoring and reporting with designated Client representative and Third Parties	X	
5. Measure, analyze, and provide management reports on performance relative to SLRs	X	
6. Develop and deliver SLR improvement plans where required	X	
7. Review and approve SLR improvement plans		X
8. Implement SLR improvement plans	X	
9. Review and approve SLR metrics and performance reports		X

2.1.4.4 Security

Security Services are the activities associated with maintaining physical and logical security of all Service Area components (e.g., hardware, Software) and data, Malware protection, access

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

19

protection and other Security Services in compliance with Client security requirements and all applicable regulatory requirements. The following table identifies Security Services roles and responsibilities that Vendor and Client shall perform.

Table 18.   Security Services Roles and Responsibilities

Security Services Roles and Responsibilities	Vendor	Client
General		
1. Provide Client security requirements and policies, and Client and other regulatory requirements		X
2. Develop, document and maintain in the Policies, Standards and Procedures Security Services standards and procedures that meet Client requirements, regulatory requirements, and adhere to Client policies	X	
3. Implement physical and logical security plans consistent with Client security policies and develop and provide documentation demonstrating adherence to the plans, processes and procedures	X	
4. Maintain a secure computing and network environment, including compliance with Client policies	X	
5. Perform information security compliance, auditing, and reporting per Client defined requirements	X	
6. Protect sensitive information (as defined by the Client), logically and physically, in storage and during transmission against unauthorized access or modification	X	
7. Review and approve Security Services standards and procedures and provide additional procedures as required		X
8. Execute security policies and provide and operate security monitoring tools including documentation demonstrating adherence to the process	X	
9. Provide, implement and manage security analysis and monitoring tools into the Client's system and network infrastructure	X	
10. Review and approve security analysis and monitoring tools		X
11. Interface, manage and coordinate, as appropriate, Vendor Subcontractors and other Third Parties (e.g., network circuit provider, Software vendors) in order to meet Client Security Services requirements	X	
Security Policy and Controls		
12. Develop, document and provide Client security strategy, policies and requirements		X
13. Facilitate Client information security awareness programs for Client employees and contingent personnel		X
14. Ensure compliance with patch management policy	X	
15. Remain up to date with current IT security trends, threats, common exploits and security best practices	X	

Security Services Roles and Responsibilities	Vendor	Client
16. Provide a Client security liaison that works with Vendor for security requirements related to the scope of this Schedule		X
17. Implement a Computer Security Incident Response Team (CSIRT) program to resolve security incidents	X	
18. Review and approve all security plans, security remediation plans, programs, and security infrastructure		X
Physical Security Control at a Vendor Managed Site		
19. Maintain controlled access to the computing areas	X	
20. Conduct review of the list of authorized people to computing areas (semi-annually)	X	
21. Place and support systems including storage media in controlled access areas	X	
System Administrative Privileges		
22. Establish access profiles and policies for adding, changing, enabling/disabling and deleting log-on access for Client and Third Parties		X
23. Manage authority/privileges for End User IDs per the established security standards		X
24. Manage application infrastructure authority / privileges	X	
25. Periodically validate the business need of users access		X
26. Disable terminated users or inactive accounts using automated processes, per Client policies		X
27. Monitor the events of administrative IDs for policy violations and events attempting avoidance of detection	X	
28. Investigate systematic attacks (e.g., attempts to logon)	X	
29. Define logging controls for user resources, according to the established security standards		X
30. Maintain logging controls for user resources, according to the established security standards	X	
31. Create reports for the following, for Vendor administrative IDs only: • Logon violations • Resource access (e.g., operating system resource access or violations) • Application and application resource access violations (e.g., programs, files, data)	X	
32. Provide logs of computer security relevant events containing sufficient data to support comprehensive audits of the effectiveness of, and compliance with security measures (audit tracking)	X	

Security Services Roles and Responsibilities	Vendor	Client
Monitoring and Incident Management		
33. Report security Incidents and violations to Client per Client policies	X	
34. Resolve security violations internal to the Client		X
35. Resolve security violations internal to Vendor	X	
36. Resolve security violations that originate outside of the hosted network(s) (e.g., denial of service attacks, spoofing, Web exploits)	X	
37. Review all security patches relevant to the IT environment and classify the need and speed in which the security patches should be installed as defined by Client security policies	X	
38. Install security patches per the Client's Change Management process and procedures including acquiring required Client approval	X	
Security Integrity Advisory		
39. Provide security advisory information in an agreed to manner	X	
40. Evaluate security advisories, assign a risk value and communicate recommended action plan to the Client	X	
Security Status Checking and Validation		
41. Provide security assessment audit focal point to define audit controls and coordinate audit activities	X	
42. Provide support for audit activities (e.g., data collection, audit tool installation, report generation)	X	
43. Develop plans to remediate audit findings that do not comply with the established Client security policies and standards	X	
44. Review and approve audit findings and remediation plans		X
45. Implement remediation plans	X	
46. Support audit activities by providing a security assessment audit coordinator to define audit controls and coordinate audit		X
47. Maintain all documentation required for security assessments, audits and internal control and control testing	X	
48. Perform semi-annual security assessments to identify control or security gaps and provide trending problem reports to the Client, and recommend remediation plan(s)	X	
49. Conduct security planning and review sessions to review results of security assessments and Vendor remediation plans	X	
50. Review and approve remediation plan(s)		X
51. Implement Client approved remediation plan(s)	X	

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

22

Security Services Roles and Responsibilities	Vendor	Client
Malware Prevention		
52. Configure and operate Malware protection Software for continuous scanning, eradication and reporting of detected Malware and Malware Incident Resolutions	X	
53. Monitor Malware websites and communicate Malware alerts	X	
54. Manage centralized anti-virus console that collects and reports on device activity, risks, infections, host IPS alerts. Develop new anti-virus installation files to support wide range of OS and platforms. Work with software deployment team to troubleshoot wide-ranging installation issues. Build and manage group containers in the centralized system to support various scan schedules, scan scope and exceptions.	X	
55. Deploy anti-Malware updates and patches following a Malware Incident per the Client Change Management procedures	X	
56. Monitor supplier information and manage up-to-date information on malicious code outbreaks and deploy the appropriate Software signature files to protect against the malicious code	X	
57. Provide automated detection and removal of malicious code using anti-Malware Software	X	
58. Promptly notify Client on detection of malicious code within the infrastructure	X	
59. Implement the established action plan and escalation procedures for a malicious code event beyond what is automatically fixed by the anti-Malware Software	X	

2.1.4.5 Asset Management

Asset Management Services are the activities associated with ongoing management and tracking of new and upgraded Service Area components (e.g., hardware, Software) in the Asset Management System. The Client currently uses InControl MasterControl Suite for IT asset management. The following table identifies Asset Management Services roles and responsibilities that Vendor and the Client shall perform.

Table 19.   Asset Management Services Roles and Responsibilities

Asset Management Services Roles and Responsibilities	Vendor	Client
1. Assume and manage an Asset Management System that meets Client requirements and adheres to Client policies (including the capability to track Assets outside of the scope of the Services)	X	
2. Manage lifecycle of all Assets from requisition ordering, inventory, installation, preventative maintenance to disposal	X	
3. Advise Client of Asset obsolescence conditions, with sufficient advance notice for the Client to make a decision regarding the replacement of the Asset (at least 18 months unless otherwise agreed to by the Client)	X	

Asset Management Services Roles and Responsibilities	Vendor	Client
4. Develop Asset type list that would be included in the Asset Management System		X
5. Review Asset type list and maintain Asset types in the Asset Management System	X	
6. Provide the Client inquiry and reporting access into the Asset Management System for all Assets including data access via a real-time access reporting portal in exportable and analyzable format and ad hoc and recurring (e.g., monthly) reports	X	
7. Input, maintain, update, track and report all in-scope Assets throughout the Asset lifecycle (i.e., acquisition to retirement)	X	
8. Maintain the accuracy of the data of in-scope Assets in the Asset Management System according to SLRs	X	
9. Provide extracts from Asset Management database for the Client to implement into its various systems	X	
10. Establish, update, and maintain the Asset database to include, at minimum, the following Asset information for each Asset: • Manufacturer • Model • Serial number • Asset identification number • Asset location • Ownership information (Vendor /Client /Third Parties - lease /purchase) • Asset cost information (e.g., current residual value, purchase price, accumulated depreciation) • Maintenance information and history including the manufacture and installation dates • Warranty information • Other billing information (e.g., lease information, Client specific information) • Transaction edit history (e.g., locations, billing and user)	X	
11. Administer and manage warranty periods for Data Center related Assets	X	
12. Administer maintenance contracts for End User Assets included in the in-scope services		X
13. Update in-scope Asset records related to all Change activities (e.g., Install/Move/Add/Change/Disposal (IMACD) activities, Break/Fix activities, enterprise reorganization and Change Management activities)	X	

Asset Management Services Roles and Responsibilities	Vendor	Client
14. Perform ongoing Asset inventories to validate that data in the Asset Management System is accurate and current and that Client has the data it requires. This activity is done at the time of refresh or when an IMACD is performed	X	
15. Provide, and upon Client approval, implement remediation plans for Asset Management System deficiencies	X	
16. Review and approve physical Asset inventory reports and remediation plans of Asset Management System		X

2.1.4.6 Software License Management

Software License Management Services are the activities associated with the acquisition, and ongoing management and tracking of Software licenses. The following table identifies the Software License Management Services roles and responsibilities that Vendor and the Client shall perform.

Table 20.   Software License Management Services Roles and Responsibilities

Software License Management Services Roles and Responsibilities	Vendor	Client
1. Manage and maintain Software licenses information through Software license lifecycle	X	
2. Conduct software vendor agreement negotiations for Client-retained contracts		X
3. Conduct software vendor agreement negotiations for non Client-retained contracts	X	
4. Review and approve software vendor agreement negotiations for non Client-retained contracts		X
5. Develop and maintain inventory of all Software licenses in a Software License Management System	X	
6. Provide the Client with online access to the Software License Management System for ad hoc queries and reports	X	
7. Report to the Client on any exceptions to vendor terms and conditions, as they occur or become known	X	
8. Coordinate and conduct Software license and maintenance agreements reviews allowing for sufficient time for negotiations prior to expiration	X	
9. Provide the Client with reports and recommendations to use in making Software acquisition and discontinuance decisions	X	
10. Provide timely and regular recommendations to purchase additional license capacity, recommending alternatives, or curtailing usage where necessary and appropriate, to restore, or continue to maintain, license compliance taking into account Client's budget cycle	X	
11. Identify and report license compliance issues	X	
12. Review license compliance issues and coordinate corrective actions		X
13. Manage and perform license audits and reconcile the number of licenses to the number of installs	X	

Software License Management Services Roles and Responsibilities	Vendor	Client
14. Provide data necessary to have the Client conduct periodic reviews and ensure that reviews are conducted 90 days prior to expiration of all Software license and maintenance agreements	X	
15. Hold periodic reviews and ensure review is conducted 90 days prior to expiration of all Software license and maintenance agreements		X
16. Obtain approval from the Client for any license change or replacement	X	

2.1.4.7 Financial/Chargeback Management and Invoicing

Financial/Chargeback Management and Invoicing Services are the activities associated with providing data that allows the Client to chargeback its internal business customers for actual usage of IT resources and to receive detailed and accurate invoices that meet Client requirements. The following table identifies the Financial/Chargeback Management and Invoicing Services roles and responsibilities that Vendor and the Client shall perform.

Table 21.   Financial/Chargeback Management and Invoicing Services Roles and Responsibilities

Financial/Chargeback Management and Invoicing Services Roles and Responsibilities	Vendor	Client
1. Define Financial/Chargeback Management and Invoicing Services requirements in sufficient detail for Vendor to provide the necessary levels of cost reporting		X
2. Develop, document, and maintain in the Policies, Standards and Procedures, Financial/Chargeback Management and Invoicing Services procedures that meet requirements and adhere to Client policies	X	
3. Review and approve Financial/Chargeback Management and Invoicing procedures		X
4. Provide chargeback reports	X	
5. Review and approve chargeback reports		X
6. Identify invoicing requirements		X
7. Document and maintain invoicing requirements	X	
8. Provide invoices per Client requirements	X	
9. Review and approve invoices, and process payments		X

2.1.5   Service Support

2.1.5.1 Incident and Problem Management

Incident and Problem Management Services are the activities associated with restoring normal Service operation as quickly as possible and to minimize the adverse impact on Client business operations, thus ensuring that the best possible levels of Service quality and Availability are maintained.

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

26

Problem Management also includes minimizing the adverse impact of Incidents and Problems on the business that are caused by errors in the Service Areas, and to prevent the recurrence of Incidents related to those errors. In order to achieve this goal, Problem Management seeks to get to the root cause of Incidents and then initiate actions to improve or correct the situation.

The following table identifies the Incident and Problem Management Services roles and responsibilities that Vendor and Client shall perform.

Table 22.   Incident and Problem Management Services Roles and Responsibilities

Incident and Problem Management Services Roles and Responsibilities	Vendor	Client
1. Establish operations and service management quality assurance and control programs	X	
2. Review and approve operations and service management quality assurance and control programs		X
3. Perform quality assurance and quality control programs	X	
4. Interface and coordinate with the Client's service desk, Client and Third Parties for Incident and Problem Management Services activities and take ownership of end to end Incident and Problem Resolution	X	
5. Provide Level 2 support and Level 3 support as required	X	
6. Establish Incident/Problem classification by priority		X
7. Establish Incident/Problem workflow, escalation, communication and reporting processes that help to achieve SLRs	X	
8. Review and approve Incident/Problem classification, prioritization and workflow, communication, escalation and reporting processes		X
9. Provide, configure, and operate an Incident and Problem Management Services tracking system that tracks Incidents across all IT Service Areas	X	
10. Provide Client access and input capabilities to Incident and Problem Management Services tracking system to allow for Incident/Problem monitoring and ad hoc reporting	X	
11. Manage entire Incident/Problem lifecycle including detection, escalation, diagnosis, Client status reporting, repair and recovery	X	
12. Ensure Incident Resolution activities conform to defined Change Management procedures	X	
13. Manage efficient workflow of Incidents including the involvement of Third Parties (e.g., Vendor, public carriers, ISP, Third Party service providers) and broadcast of Outages	X	
14. Periodically review the state of open Problems and the progress being made in addressing Problems, including Problem review sessions as required		X

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

27

Incident and Problem Management Services Roles and Responsibilities	Vendor	Client
15. Participate in Problem review sessions and provide listing and status of Problems categorized by Problem impact	X	
16. Authorize closure of Client initiated Priority 1 and 2 Incidents		X
17. Identify possible enhancement opportunities for improved operational performance and potential cost savings based on results of Incident Resolution activities	X	
18. Review and approve projects to implement enhancement opportunities		X
19. Implement approved projects to implement enhancement opportunities	X	
20. Provide known-error database and process to utilize database and provide electronic access to the Client	X	

2.1.5.2 Root Cause Analysis

Root Cause Analysis (RCA) Services are the activities associated with diagnosing and analyzing the root cause of Priority Level 1 or 2 Incidents and Problem and/or trends, and recommending and taking corrective measures to prevent the reoccurrence of such Incidents, Problems and/or trends. The following table identifies RCA Services roles and responsibilities that Vendor and Client shall perform.

Table 23. Root Cause Analysis Services Roles and Responsibilities

Root Cause Analysis Services Roles and Responsibilities	Vendor	Client
1. Conduct proactive trend analysis to identify recurring Problems and providing RCA Services trend analysis reporting to the Client	X	
2. Track and report on all Priority Level 1 and 2 Incidents and provide associated consequences	X	
3. Recommend solutions to address recurring Problems or failures	X	
4. Review and approve solutions to address recurring Problems or failures		X
5. Identify root cause of Priority Level 1 and 2 Incidents and recommend appropriate Resolution action	X	
6. Review and approve solutions to address Priority Levels 1 and 2 Incidents		X
7. Provide status report detailing the root cause of and procedure for correcting recurring Problems and Priority Levels 1 and 2 Incidents until closure as determined by the Client	X	
8. Identify root cause of Priority Level 3 and 4 Incidents at the Client's request	X	

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

28

2.1.5.3 Configuration Management

Configuration Management Services are the activities associated with providing a logical model of the Service Areas by identifying, documenting, controlling, maintaining, and verifying the installed service environment (e.g., hardware, Software, middleware, Interfaces, network). The goal of Configuration Management is to account for all IT Assets and configurations, provide accurate information on configurations and provide a sound basis for Incident, Problem, Change and Release Management Services and to verify configuration records against the infrastructure and correct any inaccuracies. The following table identifies the Configuration Management Services roles and responsibilities that Vendor and the Client shall perform.

Table 24.   Configuration Management Services Roles and Responsibilities

Configuration Management Services Roles and Responsibilities	Vendor	Client
1. Establish Configuration Management Database (CMDB), in accordance with Client requirements	X	
2. Review and approve the CMDB		X
3. Select, install and maintain Configuration Management tools	X	
4. Enter/upload configuration data into the CMDB	X	
5. Establish automated process Interfaces to Incident and Problem Management, Change Management, DR, technical support, maintenance and Asset Management processes	X	
6. Establish appropriate authorization controls for modifying configuration items and verify compliance with Software licensing	X	
7. Establish guidelines for physical and logical separation between environments (e.g., development, test and production) and the process for deploying and back out of configuration items	X	
8. Establish configuration baselines as reference points for rebuilds, and provide ability to revert to stable configuration states	X	
9. Ensure Configuration Management processes are consistent across all environments (e.g., development, test and production)	X	
10. Establish process for verifying the accuracy of configuration items, adherence to Configuration Management process and identifying process deficiencies	X	
11. Provide Client Configuration Management reports as required and defined by the Client	X	
12. Track and flag configurations that are not in conformance (e.g., exceptions list) with Client-defined standards and requirements (e.g., Client approved and unapproved non-standard configurations)	X	

2.1.5.4 Change and Release Management

Change and Release Management Services are the activities associated with ensuring that standardized methods and procedures are used for efficient and prompt handling of all Changes

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

29

and Software releases in the Client service environment (e.g., hardware, Software, middleware, Interfaces, network), in order to minimize the impact of change upon Service quality and consequently to improve the day-to-day operations of the Client environment. Change Management covers all aspects of managing the introduction and implementation of all Changes affecting all Service Areas and in any of the management processes, tools, and methodologies designed and utilized to support the Service Area components. The Change Management process includes the following process steps:

- Request process
- Recording and tracking process
- Prioritization process
- Responsibility and assignment process
- Impact and risk assessment process
- Review and approval process
- Implementation process
- Verification (test) process
- Release process
- Closure process

Release Management Services are activities associated with providing a holistic view of a Change to an existing Service or addition of new Service(s) to ensure that all aspects of a release, both technical and non-technical are considered together and to plan and oversee the successful rollout of technologies, design and implement efficient procedures for distribution and installation of Changes. The activities also ensure that only correct, authorized and tested versions are installed and that Changes are traceable and secure.

The Client has an enterprise change management board which includes representatives from both the Client and the current IT provider (SDDPC). The Client's change process includes "local change review" within the ERP Department, the IT Web Team, and SDDPC. Local reviews include both a business or functional review, followed by a technical review by SDDPC. All changes (including the development, QA/test, and production environments) must be reviewed and approved at the "local" level, including notification of potentially impacted users, before it can be forwarded for approval. Under the current process, only production system/environment changes must be approved at the enterprise level. Under this Service, the Client shall incorporate Vendor in a Change Management Board ("CCB") which includes representatives from both Parties. The purpose of the CCB is to ensure all hardware, Software, and environmental configuration changes are planned, analyzed, implemented, tested, approved, and seamlessly transitioned to a production support state. The CCB shall meet on a regularly scheduled basis to discuss and approve planned changes. Client and Vendor shall establish an agreed upon industry best practice process. Vendor shall lead the CCB for all changes occurring with/within the Vendor Services. The Client shall participate on the CCB and provide approvals. Vendor will also participate on an as needed basis with the Client on all other changes occurring outside of Vendor Services under the direction of the Client CCB.

Changes are to be tracked and integrated with configuration management, with changes requiring routine review and configurations audited for accuracy. Vendor shall provide an effective change management system that provides a high degree of control and reduces or

eliminates disruptions caused by change implementation. This system will be used for all changes to the Client environment initiated by Vendor and/or Client IT personnel.

Vendor shall provide Change and Release Management including, but not limited to the following:

- Hardware—All installations, decommissions, replacement, or other changes, and re-location of Machines in the data center, network, and in scope Service locations

- System Software—All System Software changes, including modifications to the system operating code, access methods, program products, or common system support modules

- Infrastructure Software—All infrastructure Software changes including, but not limited to, modifications to database, web server, and middleware

- Application Systems—All infrastructure related Application System changes (including changes to Software used by Vendor to fulfill the Services) being phased into the production and test environments, including governance around changes to the production and test environments. Application System changes often include alterations to processing programs, production batch jobs, addition or deletion of job steps, and implementation of new application jobs and systems

- Environment—Environmental changes involving the facilities associated with the Vendor data center and in scope Client sites. This includes items such as power, air conditioning, chilled water, raised flooring, security, motor generator, and voice and data telecommunications

The following table identifies Change Management and Release Management Services roles and responsibilities that Vendor and Client shall perform.

Table 25.   Change and Release Management Services Roles and Responsibilities

Change and Release Management Services Roles and Responsibilities	Vendor	Client
1. Provide a Change Management tool or Interface such a tool into the existing Client change management tool	X	
2. Establish and lead the CCB and conduct regularly scheduled meetings	X	
3. Participate in regularly scheduled CCB meetings		X
4. Establish Change classifications (impact, severity, risk) and Change authorization process, including a list of contacts authorized to request Changes to scope by level of authority (e.g., dollar amount impact), and any updates thereto		X
5. Administer the version control system as it relates to Release Management of Client applications		X
6. Document and classify proposed Changes to the CCB, where required risk impact and back out plans of those Changes and establish Release Management plans for major Changes	X	
7. Develop and maintain a schedule of planned Changes and provide to the Client for review as required	X	

Change and Release Management Services Roles and Responsibilities	Vendor	Client
8. Determine Change logistics	X	
9. Communicate and coordinate recommended changes with all affected parties	X	
10. Schedule and conduct Change and Release Management meetings to include review of planned Changes and results of Changes made	X	
11. Provide Change documentation as required	X	
12. Authorize and approve scheduled Changes or alter the schedule of any or all Change requests		X
13. Review Release Management details with Client and alter as appropriate (e.g., back out plan, go/no go decision)	X	
14. Notify the Client and other Third Parties of Change timing and impact	X	
15. Ensure Change and Release Management Services processes are consistent across all environments (e.g., development, test and production)	X	
16. Implement Change and adhere to detailed release plans	X	
17. Modify and update systems and documentation impacted by implemented Changes (e.g., CMDB, Asset Management System, service catalog (if applicable), DR plan)	X	
18. Verify that Change met objectives and Resolve negative impacts from the Change	X	
19. Monitor Changes and report results of Changes and impacts and provide single portal access to reports and associated logs	X	
20. Manage Change communication with the Client and Third Parties as required	X	
21. Perform quality control activities and approve Change results		X
22. Secure and maintain master copies of all in-scope Software versions in a secured Software library and update the CMDB	X	
23. Implement and document out-of-CCB-cycle Changes related to the infrastructure components	X	
24. Implement and document out-of-CCB-cycle Changes related to application software		X

3.0   Service Environment

The service environment section in each IT Service Area SOW describes and scopes a number of Service Area elements to be supported and/or with which Vendor shall comply (e.g., in scope hardware and Software). As such, this SOW shall apply to the service environment as specified in each Service Area SOW. The service environment for each Service Area shall be

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS)
Confidential Information

32

documented in the applicable SOW Appendices and are to be maintained by Vendor, reviewed with the Client, updated by Vendor and made available to the Client on a quarterly basis.

3.1.1 IT Service Management and Life Cycle Services Tools

A listing and description of all Vendor ITSM tools, associated functionality and capabilities, standard reports and associated Service Area environments supported by each tool shall be developed and maintained by Vendor in Appendix 2A.1 – IT Service Management and Life Cycle Services Tools. Over the term of the Agreement the Vendor may recommend changes to the tools, which must be mutually agreed to by the Parties before any such changes can be made by the Vendor.

4.0 Service Level Requirements

4.1 Objectives

A key objective of this outsourcing agreement is to attain Service Level Requirements (SLRs). SLRs specific to Service Areas are identified in the Service Management section of each IT Service Area SOW. SLRs applicable across all Service Areas are identified in this IT Service Management and Life Cycle Services SOW below. SLRs associated with Fee Reductions are identified in Schedule 4 – Fee Reductions. SLR performance shall be calculated based on measurements taken over the indicated Measurement Interval and reported to the Client based on the Reporting Period. SLR Fee Reductions for SLRs with multiple Measurement Intervals within the Reporting Period shall be calculated as defined in Schedule 4 – Fee Reductions. All SLRs listed below are subject to the applicable governance policies and Change Management processes and procedures.

Vendor shall provide written reports to the Client regarding Vendor's compliance with the SLRs specified in each SOW Schedule.

4.2 Service Level Requirements

Note: All times referenced are in Pacific Time.

Table 26.   Work Order Response SLR

Definition	Proposals in response to In-Scope and Out-of-Scope Client Work Orders. Vendor may elect not to respond to Out-of-Scope Client Work Orders, in which case such Work Order Responses shall not be subject to the Work Order Response SLR calculation.

SERVICE TYPE	SERVICE MEASURE	PERFORMANCE TARGET	MINIMUM PERFORMANCE %
Work Order Proposal Response (e.g., timelines, deliverables, pricing, assumptions &	Proposal delivery	10 Business Days from submission of authorized Client In-Scope or Out-of-Scope Client Work Order, or	95%

SERVICE TYPE	SERVICE MEASURE	PERFORMANCE TARGET	MINIMUM PERFORMANCE %
constraints, comprehensive and complete written documentation, required Vendor authorized approvals)		as mutually agreed to by the Parties	
	Formula	Proposal request delivered within required time/total proposals requested by the Client	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Tool	TBD	

Table 27. System Software Refresh and Updates SLRs

Definition	Vendor shall perform up to one System Software version or major release modification and unlimited service pack/maintenance/enhancement release modifications and patch modifications per year per installed system unless approved otherwise by the Client.

System Software Refresh and Updates Service Level Requirements			
Software Refresh and Updates	**Service Measure**	**Performance Target**	**SLR Performance %**
Deploy Emergency Maintenance Release (e.g., security pack, bug patch, antivirus, anti-SPAM, and anti-Spyware update deployments)	Time to deploy	Perform same Business Day as signoff	99.0%
Deploy Non-Emergency Maintenance Release (e.g., Version 8.1.5 to Version 8.1.6)	Time to Deploy	Perform within the next regular maintenance time window	99.0%

System Software Refresh and Updates Service Level Requirements			
Software Refresh and Updates	**Service Measure**	**Performance Target**	**SLR Performance %**
Implementation of Enhancement Release (e.g., Version 8.1 to Version 8.2)	Time to deploy	Within 60 Business Days after notification by Client or per Client approved project schedule	98.0%
Implementation of Major Release Updates (e.g., Version 8 to Version 9)	Time to deploy	Within 120 Business Days after notification by Client or per Client approved project schedule	98.0%
	Formula	Number of events completed on time/total of events occurring during Measurement Interval	
	Measure Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Tool	TBD	

Table 28. System/Security Administration SLRs

System/Security Administration Service Level Requirements			
System Administration Task	**Service Measure**	**Performance Target**	**SLR Performance %**
Proposal for Security Remediation Following Discovery of a Security Risk (e.g., timelines, deliverables, assumptions & constraints, comprehensive and complete written documentation)	Proposal delivery	2 Business Days	97%
	Formula	Number of events completed within performance target /events occurring during Measurement Interval	
	Measurement Interval	Monthly	

System/Security Administration Service Level Requirements			
System Administration Task	**Service Measure**	**Performance Target**	**SLR Performance %**
	Reporting Period	Monthly	
	Measurement Tool	TBD	

Table 29.   Incident Resolution SLRs

Definition	Time to Resolve Incidents following responses to different Incident Priority Level classifications. Time to respond as used in this SLR means Vendor's notification of the Incident to the Client-designated contact(s) via phone, text message or email. The time to respond measurement shall begin once the Vendor becomes aware of the Incident.

Incident Resolution SLRs			
Incident Resolution	**Service Measure**	**Performance Target**	**SLR Performance %**
Priority 1 – Business Hours	Time to respond	< 15 minutes	95.0%
Priority 1 – Public Safety (24x7x365)	Time to respond	<15 minutes	95%
Priority 1 – Non-Business Hours	Time to respond	< 30 minutes	95%
Priority 2	Time to respond	< 30 minutes	95%
Priority Level 1	Time to Resolve	< 4 hours < 8 hours	95.0% 98.0%
Priority Level 2	Time to Resolve	< 8 hours < 16 hours	95.0% 98.0%
Priority Level 3	Time to Resolve	< 3 Business Days or within an agreed upon time frame	95.0%
Priority Level 4	Time to Resolve	< 5 Business Days or within an agreed upon time frame	95.0%

Incident Resolution SLRs			
Preliminary Root Cause Analysis Report via Email	Time to report	Within 3 Business Days of Incident Resolution for Priority Level 1 or as otherwise requested by the Department of IT for Priority 2 Incidences	95.0%
Formal Root Cause Analysis	Time to report	Within 5 Business Days of Incident Resolution for Priority Level 1 or as otherwise requested by the Department of IT for Priority 2 Incidences	95.0%
	Formula	Number of events resolved within Performance Target/Total of all requests occurring during Measurement Interval	
	Measurement Interval	Weekly	
	Reporting Period	Monthly	
	Measurement Tool	TBD	

Table 30.   Priority Levels Matrix

		IMPACT		
		High	**Medium**	**Low**
U R G E N C Y	**High**	Priority 1	Priority 2	Priority 3
	Medium	Priority 2	Priority 3	Priority 4
	Low	Priority 3	Priority 4	Service Request

Table 31.   Priority Level Definitions

Priority Level	Description
1 - Emergency/Urgent	The Problem has caused a complete and immediate work stoppage affecting a primary business process or a broad group of End Users such as an entire department, floor, branch, line of business, or external customer. No Workaround is available. Examples: Major application Problem (e.g., ERP, Exchange, etc.) Severe Problem during critical periods (e.g., month-end processing) Security Violation (e.g., denial of service, widespread virus, etc.) After Hours Incidents generated from Client Public Safety Personnel (e.g., Police, Fire)
2 - High	A business process is affected in such a way that business functions are severely degraded, multiple End Users are impacted or a key customer is affected. A Workaround may be available; however the Workaround is not easily sustainable. Examples: Failure of single host supporting ERP dialog instances or BO reporting. Services are still available on other hosts but response times are severely degraded and batch processing window increased. Storage system issue impacting access times to file shares.

3 - Medium	A business process is affected in such a way that certain functions are unavailable to End Users or a system and/or service is degraded. A Workaround may be available.
	Examples:
	    Personal productivity Problem (e.g., local workstation or printer, PDA)
	    Redundant system problem

4 - Low	An Incident that has little impact on normal business processes and can be handled on a scheduled basis. A Workaround is available. Examples: Preventative Maintenance

4.2.1 Backup and Restore Requirements

Vendor shall implement and maintain backup and restoration capabilities for specified Service Area data, applications and component configurations as defined in each Service Area SOW. Vendor shall perform error and omission free incremental backups, full backups and full archive backups according to the Backup Schedule presented below. Recovery procedures shall be capable of restoring Service delivery for failed Service Area data, applications and component configurations according to the Restoration SLRs listed below. Service Area components requiring scheduled backups shall be referenced in the service environment section of each Service Area SOW.

Vendor shall continually monitor backup jobs and immediately identify and fix any failures to ensure successful reruns to meet frequency requirements. Such timely reruns shall be considered as successful completion of the SLR.

Table 32. Backup Schedule

Backup Schedule SLRs					
Type of Backup	**Backup Frequency**	**Storage Site**	**Retention/Purge Period**	**Target**	**SLR Performance %**
Incremental	Daily	On-site (with copy off-site)	35 days	Backup frequency	98%
Full (Backup)	Weekly	Off-site	12 weeks	Backup frequency	100%
Full (Archive)	Monthly	Off-site	6 months	Backup frequency	100%
All				Quarterly Successful test of each type of backup restore process	100%
	Formula		Number of backups completed on schedule/total of all backups scheduled during Measurement Interval		
	Measurement Interval		Monthly		
	Reporting Period		Monthly		
	Measurement Tool		TBD		

Table 33.   Restoration SLRs

Restoration Service Level Requirements			
Restoration Type	**Service Measure**	**Performance Target**	**SLR Performance %**
Production Data Restore Requests (unless otherwise planned as a prescheduled event) (excludes requests where the restoration method or size will not support the Performance Target)	Commencement time for data 1 week old or less	$\leq$ 2 Business hours from Client request	95%

Restoration Service Level Requirements			
Test/Volume Backup Restore Requests (unless otherwise planned as a prescheduled event) (excludes requests where the restoration method or size will not support the Performance Target)	Commencement time for data 1 week old or less	$\leq$ 8 Business hours from Client request	95%
Volume Back Ups Restore Requests	Completion time for data > than 1 week old	Commence restore within 3 Business Days	95%
	Formula	Number of requests completed within performance target /total of all requests occurring during Measurement Interval. Successful tests will not include corrupt or open files. This will allow for the possibility of a current OS not allowing a backup of a particular file, or the file is already corrupted.	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Tool	TBD	

4.2.2   Asset Tracking and Management

Definition	Within five (5) Business Days after the first Business Day of each calendar quarter, Vendor shall select a statistically valid sample, based on the approved Asset management report and in accordance with the process specified in the Policies, Standards and Procedures Manual, to measure Vendor's compliance with the following SLRs pertaining to the accuracy of individual data elements that are electronically discoverable or updated as part of a change management process in the Asset tracking database. Accuracy of data shall adhere to the following SLR.

Table 34.   Asset Tracking SLR

Schedule 2A – IT Service Management and Life Cycle SOW to MSA for IT Services (City of San Diego and AtoS) Confidential Information
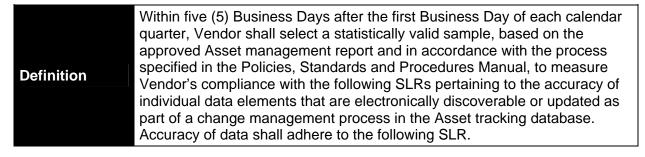
40

Asset Tracking Service Level Requirements			
Asset Tracking Accuracy	Accuracy	Accuracy percentage of each of the following data elements as determined by sample:	
		Data Element	**Accuracy Percentage**
		Serial number	97%
		Location	97% for assets located within the primary data center or approved data sites
			Best Effort for assets at all other locations
		Hardware/software configuration	97%
	Formula	Number of tracked Assets where data element is determined to be correct/total number of tracked Assets sampled	
	Measurement and Reporting Interval	Quarterly	
	Measurement Tool	TBD	

4.2.3   End User Satisfaction Survey

Definition	The Client shall establish an End User satisfaction survey, which shall be facilitated by the Client or a Client-designated Third Party, with assistance from the Vendor. The survey shall query all Client employee End Users that are eligible to use the Services and have a Client e-mail account.
	The Client shall gather, analyze, and evaluate the results of the survey, and such results shall be reviewed with the Vendor. Upon delivery of the results, the Parties shall meet to jointly identify any areas of End User dissatisfaction. The Vendor shall prepare a project plan with Client's input and approval to Resolve End User dissatisfaction.

Table 35.   End User Satisfaction SLRs

End User Satisfaction SLRs			
Customer Satisfaction	**Service Measure**	**Performance Target**	**SLR Performance %**
End User Scheduled Survey (conducted semi-annually)	End User Satisfaction	End Users responding should be very satisfied or satisfied	90%

End User Satisfaction SLRs			
Client Program Management	Program Management Satisfaction	Those responding should be very satisfied or satisfied	90%
	Formula	Sum of survey result from each participant/total number of participants responding to scheduled survey	
	Measurement Interval	Semi-annually	
	Reporting Period	Semi-annually	
	Measurement Method/Source Data	TBD	

4.3   Reports

Vendor shall provide written reports to Client regarding Vendor's compliance with the SLRs specified in this Section and other management reports. Reports are required per the following:

Table 36.   Reports

Report Description	Timing
Full list TBD with selected Vendor – see examples below	
Asset Management Activity Summary	Monthly
SAP Lifecycle Management	Monthly
Project Status	Weekly
Monthly PMO Summary	Monthly
Work Order Summary	Weekly
Security Events and Response Summary	Weekly
Maintenance Activity	Monthly
TR&R Activity	Quarterly
Service Area Capacity Status and Trending	Quarterly
Backup Schedule and Backups Performed	Weekly, Monthly
SLR Report	Per SLR Schedule
Chargeback Report	Monthly
Incident and Problem Activity and Resolution	Weekly, Monthly
RCA Summary Report	Monthly
Scheduled and Implemented Change Report	Weekly
Configuration Management Report	Monthly
Monthly Dashboard Report	Monthly
Daily Security Report	Daily, Monthly
SSAE16 Report	Annual

5.0 List of Referenced MSA Schedules and Attachments

MSA Schedule / Attachment	Description
Schedule 2B	Data Center Services SOW
Schedule 2C	Service Desk Services SOW
Schedule 2D	Desktop Support Services SOW
Schedule 3	Fees
Schedule 4	Fee Reductions
Attachment I	Technology Refresh Plan
Attachment J	Reports