



Other Government Entity (OGE) Service Catalog

South Carolina Department of Administration
Division of Technology Operations (DTO)
Statewide Contract: 4400040058

October 1, 2026

Smartronix, LLC (SMX)
44150 Smartronix Way, Suite 200
Hollywood, MD 20636-3172

1. Purpose

This Service Catalog describes the cloud, managed service, technical support, professional service, migration, implementation, and optional service capabilities available to eligible Other Government Entities under the South Carolina Managed Cloud Services Contract.

This catalog should be used with the OGE Pricing Guide, executed statewide contract, applicable contract exhibits, ordering instructions, and project-specific Statement of Work or Quote. The executed contract and incorporated exhibits govern in the event of a conflict.

This Service Catalog describes the cloud, managed service, technical support, professional service, migration, implementation, and optional service capabilities available to eligible Other Government Entities under the South Carolina Managed Cloud Services Contract.

Summary of Services:

Service Category	Description
Cloud Services	Infrastructure, platform, and cloud-native services via leading CSPs
Managed Services	24x7 operational management, monitoring, and support
Technical Support	Engineering, troubleshooting, escalation, and service management
Professional Services	Consulting, architecture, and advisory delivered through the RFS process
Migration Services	Planning and execution of workload and data migrations to the cloud
Implementation Services	Deployment, configuration, testing, and stabilization
Optional Services	Security, optimization, governance, AI/analytics, and specialized engineering

The executed contract and incorporated exhibits govern in the event of a conflict.

2. Request for Solution (RFS) Services

The Request for Solution (RFS) process is used for project-specific consulting, assessment, architecture, migration, modernization, implementation, optimization, engineering, and related professional services. RFS complexity, scope, deliverables, staffing, schedule, assumptions, and pricing are documented in the SOW before work begins. Simple projects may result in a Quote which will contain only the applicable content.

RFS Services Available

Service Area	Description
Cloud Readiness	Assessment of current infrastructure, applications, and readiness for cloud adoption
Cloud Strategy	Structured approach for adopting, expanding, governing, or optimizing cloud services
Cloud Architecture	Design of foundational architecture, solution blueprints, and infrastructure patterns
Landing Zones	Foundational account, network, identity, security, and governance structure implementation
Migration	Planning and execution of workload rehosting, replatforming, and relocation
Modernization	Containerization, serverless, API enablement, and DevSecOps implementation
Security Architecture	IAM, encryption, monitoring, and compliance-aligned security design
Disaster Recovery	HA/DR planning, RTO/RPO analysis, and failover procedures
Hybrid Cloud	Connectivity design, identity federation, and shared security controls
Multi-Cloud Integration	Cross-platform workload placement, monitoring, and governance
Infrastructure Modernization	Platform upgrades, automation, and cloud-native service adoption
Optimization	Rightsizing, cost analysis, reserved capacity planning, and architecture efficiency
Database Projects	Database migration, modernization, performance, and operational support
Network Projects	Connectivity, routing, firewall, and network administration
Cloud Governance	Policy, tagging, cost standards, CCoE support, and automation frameworks
AI-Supporting Architecture	Data platforms, ML infrastructure, and cloud services supporting AI/analytics workloads
Specialized Engineering	Custom engineering, integration, and technical advisory engagements

3. How Services Are Acquired / Statement of Work

An OGE begins by identifying its desired business outcome, current technical environment, preferred cloud platform, anticipated workloads, security requirements, service levels, implementation schedule, and available budget. SMX and the OGE then conduct discovery to determine the appropriate service combination. The resulting solution is documented in a project-specific Statement of Work.

Discovery Process

Step	OGE Identifies / SMX Supports
Business Objectives	Desired outcomes, operational drivers, and organizational priorities
Environment	Current technical environment, platforms, and existing cloud footprint
Workloads	Applications, data, and infrastructure to be migrated or managed
Security	Applicable compliance requirements, data classifications, and security controls
Service Levels	Availability, response time, and support expectations
Schedule & Budget	Implementation timeline, milestones, and funding parameters

SOW Contents

Category	SOW Element	Description
Scope	Scope and objectives	Project boundaries, goals, and success criteria
Technical	Selected CSP	AWS, Azure, Google Cloud, or OCI selection
Technical	Workloads and environments	Applications, data, and environments in scope
Services	Managed service components	Specific managed services and service scope
Services	Optional services	Additional services selected by the OGE
Governance	Roles and responsibilities	SMX and OGE responsibilities and decision rights
Delivery	Deliverables and acceptance criteria	Defined outputs and approval standards
Compliance	Security and compliance requirements	Applicable laws, regulations, and policies
Performance	Service levels	SLAs, availability targets, and response commitments

Category	SOW Element	Description
Schedule	Schedule and milestones	Project phases, timelines, and key milestones
Financial	Pricing assumptions	Scope assumptions underlying the cost estimate
Financial	Estimated CSP consumption	Projected cloud resource usage and cost estimates
Financial	Applicable contract rates	Rates per the OGE Pricing Guide
Financial	Billing and invoicing terms	Invoice timing, formats, and payment procedures
Governance	Change-control procedures	Process for managing scope and cost changes

⚠ Important:

No project-specific work should begin until the OGE has completed its required internal review, approved the SOW, and issued the appropriate purchasing instrument.

4: Cloud Planning and Readiness Services

4.1 Cloud Readiness Assessment

The Cloud Readiness Assessment evaluates the OGE's current infrastructure, applications, operational model, security posture, staffing, governance, costs, technical dependencies, and readiness for cloud adoption.

Deliverable	Description
Current-state inventory	Documented catalogue of existing infrastructure, applications, and services
Application & workload assessment	Evaluation of application suitability and migration complexity
Cloud suitability analysis	Determination of cloud-fit for each workload and service
Dependency findings	Technical, operational, and integration dependencies identified
Risk register	Identified risks, likelihood, impact, and mitigation recommendations
Migration-wave recommendations	Suggested sequencing and prioritization of workloads for migration
High-level target architecture	Initial architectural vision aligned to OGE requirements

Deliverable	Description
Preliminary cost model	Initial estimates for CSP consumption and service costs
Cloud adoption roadmap	Phased plan for cloud adoption with milestones and timelines

4.2 Cloud Strategy Development

Cloud Strategy Development establishes a structured approach for adopting, expanding, governing, or optimizing cloud services.

Deliverable	Description
Cloud vision and objectives	Defined strategic intent and measurable goals for cloud adoption
Business-case analysis	Financial and operational justification for cloud investment
Provider-selection criteria	Framework for evaluating and selecting cloud service providers
Operating-model recommendations	Guidance on team structure, processes, and governance for cloud operations
Governance framework	Policies, standards, and controls for cloud resource management
Security & compliance considerations	Applicable regulatory and security requirements mapped to cloud approach
Financial-management approach	FinOps strategy, tagging, cost allocation, and budget management
Migration & modernization roadmap	Sequenced plan for moving workloads and adopting cloud-native services
Organizational readiness	Skills assessment, training needs, and change management recommendations

4.3 Cloud Cost Assessment and Forecasting

SMX may develop estimates based on workload characteristics, projected consumption, service architecture, storage, network traffic, licensing, managed support, and optional service requirements. Actual CSP charges remain consumption-based and may vary from estimates.

5: Cloud Architecture and Engineering

5.1 Landing Zone Design and Implementation

A cloud landing zone establishes the foundational architecture through which the OGE deploys and governs workloads.

Service Component	Description
Account/subscription structure	Account, subscription, project, or tenancy hierarchy and naming standards
Identity integration	Directory services, SSO, and federated identity configuration
Network topology	VPC/VNet design, subnetting, routing, and connectivity architecture
Segmentation	Network segmentation, micro-segmentation, and zone design
Logging and monitoring	Centralized logging, audit trails, and operational monitoring baseline
Security controls	Baseline security configurations, guardrails, and policy enforcement
Resource tagging	Tagging strategy for cost allocation, governance, and operational management
Baseline automation	Infrastructure-as-code templates and deployment automation
Governance controls	Service control policies, compliance policies, and exception management

5.2 Solution Architecture

Solution Architecture services translate business and technical requirements into an implementable cloud design.

Service Component	Description
Requirements analysis	Business and technical requirements gathering and documentation
Architecture alternatives	Comparative options analysis with trade-offs and recommendations
Availability design	Multi-AZ, multi-region, and redundancy architecture
Scalability design	Auto-scaling, elasticity, and capacity planning architecture
Security architecture	Defense-in-depth, identity, encryption, and monitoring design
Integration design	API, messaging, event-driven, and data integration patterns
Backup & DR design	Backup strategies, recovery objectives, and failover architecture
Architecture documentation	Decision records, diagrams, and architecture artifacts

5.3 Infrastructure Architecture

Infrastructure Architecture services address compute, storage, operating systems, virtualization, networking, observability, resiliency, and platform dependencies.

5.4 Hybrid and Multi-Cloud Architecture

Hybrid and multi-cloud services support environments that combine on-premises systems with one or more CSP platforms.

Service Component	Description
Connectivity design	VPN, dedicated interconnect, and SD-WAN connectivity architecture
Identity federation	Cross-platform identity and authentication integration
Shared security controls	Consistent security posture across on-premises and cloud environments
Workload placement	Decision framework for on-premises vs. cloud vs. multi-cloud placement
Data exchange	Data transfer, synchronization, and integration patterns
Monitoring integration	Unified observability across hybrid and multi-cloud environments
DR design	Disaster recovery spanning on-premises and cloud platforms
Cross-platform governance	Policies and controls applied consistently across all platforms

6: Migration and Implementation Services

6.1 Migration Planning

Planning Component	Description
Application discovery	Inventory and characterization of applications to be migrated
Dependency mapping	Identification of technical and operational dependencies between systems
Migration classification	Categorization of workloads (rehost, replatform, refactor, relocate)
Wave planning	Sequenced grouping of workloads into migration waves
Cutover strategy	Planned approach for production cutover with minimal downtime
Rollback planning	Documented rollback procedures for each migration wave
Testing strategy	Validation and acceptance testing approach for migrated workloads
Risk mitigation	Identified risks and mitigation plans for each migration phase

6.2 Workload Migration

Services may include rehosting, replatforming, relocating, refactoring support, data migration, database migration, testing, cutover, and post-migration stabilization.

6.3 Data and Database Migration

Services may include structured data, unstructured data, database engines, replication, transfer, validation, performance, integrity, security, and cutover.

6.4 Application Modernization

Modernization Type	Description
Containerization	Docker/Kubernetes containerization for cloud-native deployment
Serverless architecture	Event-driven, function-based architecture adoption
Platform-service adoption	Migration to managed CSP platform services (PaaS)
Database modernization	Migration to cloud-native or managed database services
API enablement	REST/GraphQL API implementation and API gateway integration
DevSecOps implementation	CI/CD pipelines, automated testing, and security integration
Automation	Infrastructure-as-code and operational automation implementation
Cloud-native integration	Integration with CSP-native messaging, event, and workflow services

6.5 Implementation and Stabilization

Services may include configuration, deployment, testing, documentation, training, transition to operations, and a defined stabilization support period following go-live.

7: Cloud Service Provider (CSP) Services

SMX supports cloud services delivered through leading cloud service providers. CSP charges are based on actual eligible consumption. Applicable contract discounts and limitations are described in the OGE Pricing Guide. Third-party marketplace products or other products as defined (e.g., emerging AI services) will not receive a discount when SMX does not receive a corresponding discount.

Cloud Service Provider	Abbreviation	General Service Availability
Amazon Web Services	AWS	Infrastructure, platform, data, security, networking, storage, application, analytics, and cloud-native services
Microsoft Azure	Azure	Infrastructure, platform, data, identity, security, networking, productivity integration, analytics, and cloud-native services

Cloud Service Provider	Abbreviation	General Service Availability
Google Cloud	Google Cloud	Infrastructure, platform, data, analytics, machine learning, security, networking, and cloud-native services
Oracle Cloud Infrastructure	OCI	Infrastructure, database, application, networking, storage, security, and cloud-native services

Cloud Consumption Services

Cloud consumption services may include compute, storage, databases, backup, networking, security products, monitoring, platform services, middleware, development services, analytics, and other eligible CSP offerings.

8: Managed Cloud Services

Managed Cloud Services provide operational management for the applicable CSP. Pricing is determined by the applicable monthly CSP consumption tier while the scope of services is defined by the Statement of Work. The selected services, service hours, response expectations, exclusions, dependencies, and customer responsibilities must be identified in the SOW.

Managed Service	Description
24x7 Monitoring	Continuous monitoring of cloud infrastructure, services, and workloads
Event & Alert Management	Detection, triage, and response to operational events and alerts
Incident Management	Structured process for identification, classification, and resolution of incidents
Service Request Fulfillment	Processing of standard and approved service requests
OS Administration	Operating system configuration, maintenance, and routine administration
CSP Platform Administration	Management of CSP services, configurations, and resource lifecycle
Identity & Access Support	IAM support for user accounts, roles, policies, and access reviews
Backup Monitoring	Monitoring of backup jobs and alerting on failures or anomalies
Patch Coordination	Coordinating OS and infrastructure patching in alignment with OGE policies

Managed Service	Description
Capacity Monitoring	Tracking resource utilization trends and flagging capacity thresholds
Performance Analysis	Analysis of performance data and identification of degradation patterns
Operational Reporting	Regular reports covering availability, incidents, performance, and service metrics
Technical Support	Tiered technical support for cloud platform and managed service issues
Escalation Management	Structured escalation to CSP, senior engineers, or specialized teams
Service Management	Customer success management, QBRs, and ongoing relationship management
Configuration Support	Assistance with CSP service configuration changes and updates
Cloud Cost & Usage Visibility	Visibility into CSP consumption, cost trends, and usage reporting

9: Security and Compliance Services

Security and Compliance Services provide design, implementation, and operational support for OGE security requirements across cloud environments.

Security Service	Description
Security architecture	Defense-in-depth and zero-trust architecture design for cloud environments
Identity & access management	IAM design, least-privilege, role-based access, and privileged access management
Role & privilege design	Role definitions, privilege boundaries, and separation-of-duties controls
Security logging	Centralized log collection, retention, and audit trail management
Monitoring integration	SIEM integration, alert configuration, and security event correlation
Vulnerability management	Coordination of scanning, assessment, and remediation activities
Configuration review	Baseline configuration assessment against security standards and benchmarks

Security Service	Description
Encryption design	Encryption-at-rest and in-transit design, key management strategy
Network security	Firewall rules, security groups, WAF, and network access controls
DDoS protection	Configuration and management of DDoS protection services
Security incident coordination	Incident detection, containment, and response coordination
Compliance evidence support	Documentation and evidence collection for audits and assessments
Policy-alignment support	Mapping security controls to applicable laws, regulations, and policies

OGE Responsibility:

The OGE remains responsible for identifying applicable laws, regulations, policies, data classifications, institutional requirements, contractual obligations, records-retention requirements, and industry standards.

10: Network Services

Service	Description
Customer-to-CSP Connections	Planning and implementation support for dedicated or VPN connectivity between the OGE and the cloud environment (10.1)
Networking Within CSPs	Configuration or management of networking components within AWS, Azure, Google Cloud, or OCI (10.2)
Customer Virtual CSP Connections	Virtual connectivity between OGE resources and CSP environments, subject to CSP capabilities and approved design (10.3)
Network Administration	Network configuration, routing, firewall coordination, connectivity testing, monitoring, availability support, capacity analysis, and troubleshooting (10.4)

11: Virtual Machine Services

11.1 Virtual Machine System Administration

Service Component	Description
OS configuration	Initial and ongoing operating system configuration and hardening
Routine administration	Day-to-day VM management, maintenance, and operational support

Service Component	Description
Account support	Local account management, privilege review, and access control support
Patch support	OS patch assessment, testing, and coordinated deployment
Capacity review	VM sizing analysis and recommendations for rightsizing
Performance review	CPU, memory, disk, and network performance analysis
Incident support	Troubleshooting, diagnosis, and resolution of VM incidents
Backup coordination	Backup scheduling, monitoring, and recovery validation
Configuration documentation	Maintenance of current configuration records and change history

11.2 Virtual Machine Middleware Services

Services may include installation, configuration, maintenance, monitoring, administration, and troubleshooting for approved middleware products hosted on virtual machines. The SOW should identify the specific product, environment, support responsibility, configuration scope, and service boundary.

12: Cloud-Native Middleware Services

Cloud-Native Middleware Services support approved CSP-native integration, messaging, application runtime, workflow, API, event-processing, or related platform products.

Service Type	Examples / Description
Integration services	CSP-native integration platforms and middleware (e.g., API gateways, service meshes)
Messaging services	Managed queuing, pub/sub, and event streaming services (e.g., SQS, Service Bus, Pub/Sub)
Application runtime	CSP-managed application hosting and runtime environments (e.g., App Service, Cloud Run)
Workflow services	Orchestration and workflow automation services (e.g., Step Functions, Logic Apps)
Event-processing services	Event-driven processing and stream analytics (e.g., Kinesis, Event Hubs)

The SOW should identify the specific product, environment, support responsibility, configuration scope, and service boundary.

13: Database Management Services

The supported database engine, instance count, environment, operating model, service hours, and responsibility boundaries must be documented in the SOW.

Service Component	Description
Database administration	Day-to-day DBA activities, maintenance, and lifecycle management
Monitoring	Database performance, availability, and error condition monitoring
Backup & recovery coordination	Backup scheduling, monitoring, restore testing, and recovery procedures
Performance analysis	Query optimization, index management, and performance tuning
Capacity management	Storage growth forecasting, scaling recommendations, and resource planning
Patch coordination	Database engine patch assessment, testing, and coordinated deployment
Security support	Database access controls, encryption, and audit log management
Availability support	High-availability configuration, failover testing, and uptime management
Data-integrity support	Consistency checks, data validation, and integrity monitoring
Operational documentation	Run books, configuration records, and operational procedures

14: DDoS Protection Services

DDoS Protection Services provide managed support for eligible protected resources and may include configuration, monitoring integration, alert handling, escalation, and service coordination. CSP charges for underlying DDoS products or services may apply separately.

Service Component	Description
Configuration	DDoS protection service configuration for eligible protected resources
Monitoring integration	Integration with monitoring tools for DDoS event detection and visibility
Alert handling	Response to DDoS alerts and event notifications
Escalation	Escalation to CSP DDoS response teams when required
Service coordination	Coordination of protective actions and post-event analysis

15: Backup, Recovery, and Resiliency

The OGE must approve retention, recovery, availability, data-protection, and testing requirements.

Service Component	Description
Backup architecture	Design of backup strategy, scope, and technology selection
Backup configuration	Implementation of backup policies, schedules, and targets
Backup monitoring	Continuous monitoring of backup job status and alerting on failures
Retention configuration	Configuration of retention policies aligned to OGE requirements
Restore testing	Scheduled restoration tests to validate backup integrity and recoverability
Recovery procedure development	Documented recovery procedures and run books
High-availability design	Multi-AZ and multi-region availability architecture
Disaster-recovery planning	DR plan development, tabletop exercises, and documentation
RTO/RPO analysis	Recovery time and recovery point objective analysis and validation
Failover and recovery exercises	Planned DR exercises and live failover validation

16: Cloud Optimization Services

Recommendations do not guarantee a specific amount of savings because actual results depend on consumption, workload behavior, CSP pricing, service changes, and OGE implementation decisions.

Optimization Area	Description
Resource utilization	Analysis of compute, storage, and service utilization patterns
Rightsizing opportunities	Identification and recommendation of appropriately sized resources
Idle/unused resources	Detection and remediation of idle or abandoned cloud resources
Storage tiering	Recommendations for cost-effective storage tiers and lifecycle policies
Reserved/committed-use options	Analysis of Reserved Instances, Savings Plans, and committed-use discounts
Architecture efficiency	Architectural pattern recommendations to reduce cost and improve performance

Optimization Area	Description
Licensing considerations	License optimization, BYOL opportunities, and CSP-provided alternatives
Tagging & cost allocation	Cost allocation through consistent resource tagging and reporting
Budget alerts	Proactive cost anomaly detection and budget threshold alerting
Operational efficiency	Process and automation recommendations to reduce operational overhead

17: Cloud Governance and Cloud Center of Excellence Support

Service Component	Description
Governance-model development	Design of cloud governance operating model, roles, and processes
Cloud policy development	Development of cloud use policies, standards, and guardrails
Account & subscription standards	Naming conventions, hierarchy standards, and account management practices
Architecture standards	Reference architectures, patterns, and approved service standards
Security guardrails	Preventive and detective controls implemented as policy-as-code
Cost-management standards	Budget governance, showback/chargeback, and FinOps practices
Resource tagging	Mandatory tagging standards for cost, compliance, and operations
Exception processes	Formal exception review, approval, and documentation procedures
CCoE support	Cloud Center of Excellence team support, enablement, and tooling
Automation & DevOps frameworks	IaC templates, pipeline standards, and automation frameworks
Tool integration	Integration of governance tools with ITSM, CMDB, and monitoring platforms
Product orchestration	Service catalog, self-service provisioning, and product management

18: Artificial Intelligence and Advanced Analytics Services

Where permitted under the contract and applicable purchasing requirements, an RFS may address cloud infrastructure, data platforms, security architecture, implementation support, governance controls, or other technical services supporting AI, machine learning, generative AI, analytics, or intelligent automation.

RFS Identification Requirements for AI Engagements

Required Element	Description
Proposed business purpose	Clear description of the business problem or objective being addressed
Intended users	Who will use or be impacted by the AI system or service
AI capabilities	Specific AI/ML features, models, or services to be used
Data sources	Input data types, sources, volumes, and data flows
Data classifications	Sensitivity, PII, regulated data, and data handling requirements
Model / service provider	Model origin, third-party service provider, and licensing terms
Training-data considerations	Training data sources, bias considerations, and data provenance
Human-oversight requirements	Required human-in-the-loop controls and review processes
Security controls	Security requirements specific to AI/ML workloads and pipelines
Privacy requirements	Data privacy obligations, consent, and anonymization requirements
Records-retention	Retention requirements for AI outputs, logs, and decision records
Intellectual property	IP ownership of models, outputs, and training data
Accessibility	ADA/WCAG accessibility requirements for AI-powered interfaces
Performance measures	Defined metrics for measuring AI system accuracy and effectiveness
Risk controls	Risk mitigation measures, monitoring, and model governance
Institutional approvals	Required internal AI governance, ethics, and procurement approvals



Artificial Intelligence Purchasing Review

If the proposed acquisition includes artificial intelligence (AI), generative AI, machine learning, intelligent automation, or cloud services supporting AI workloads, institutions of higher education should review applicable Department of Administration Artificial Intelligence Center of Excellence (AI CoE) guidance and institutional AI governance requirements before submitting a Request for Solution or approving a Statement of Work.

19: Services Requiring Additional Definition

The following service elements must be specifically defined in the applicable Statement of Work. These items are not presumed to be included merely because a general service category appears in this catalog.

Element Requiring SOW Definition	Element Requiring SOW Definition
Exact products and workloads in scope	Security controls and configurations
Service hours and coverage windows	Compliance obligations and evidence requirements
Service levels and SLA targets	Accessibility requirements
Response and restoration objectives	Training and knowledge transfer requirements
Included incident and request types	Documentation deliverables
CSP consumption estimates	Travel and on-site service requirements
Licensing (OS, middleware, database)	Customer resource commitments
Third-party products and services	Acceptance criteria and deliverable standards
Data migration volumes and timelines	Transition and termination activities

20. SMX Support

SMX provides comprehensive support services throughout the lifecycle of your engagement:

Support Service	Description
Service Desk	Single point of contact for all service requests and support inquiries
Incident Management	Structured end-to-end process for detecting, recording, and resolving incidents
Problem Management	Root cause analysis and permanent resolution of recurring incidents
Change Management	Controlled process for evaluating, approving, and implementing changes
Technical Support	Tiered technical expertise for platform, infrastructure, and cloud service issues
Escalation Management	Structured escalation to senior engineers, CSP support, or specialized teams
Customer Success Management	Dedicated customer success manager for account oversight, QBRs, and relationship management

21. Need Assistance?

SMX can assist your organization at any stage of the procurement and implementation process:

Assistance Area	How SMX Can Help
Project planning	Development of implementation roadmaps, phasing, and project frameworks
Budget estimates	Preliminary cost modeling and consumption estimates to support funding requests
Technical architecture	Pre-sales architecture reviews and design recommendations
Scope development	Assistance developing the scope of work for RFS or SOW submissions
Cloud assessments	Readiness assessments to evaluate cloud fit and migration complexity
Service recommendations	Guidance on selecting appropriate services from the catalog for your needs

Contact Information

To learn more about services available under this contract, initiate a Request for Solution, or obtain assistance with ordering, contact the SMX State and Local Account Team / Program Management Office:

	Contact 1	Contact 2
Name	Shelly Reade	Elizabeth Brown
Title	Sr. Director, SLED	SC MCS Account Manager
Email	sreade@smxtech.us	etbrown@smxtech.us
Website	www.smxtech.com	

Important Notice

This document provides general guidance and does not replace the executed Statewide Contract, incorporated exhibits, applicable amendments, or the Pricing Guide. In the event of a conflict between this document and the contract, the executed contract and incorporated exhibits govern.