

MASTER SERVICES AGREEMENT

between

TEXAS EDUCATION AGENCY

and

SKYWARD, INC.

JUNE 1, 2011

EXHIBIT A-5

NETWORK SERVICES

STATEMENT OF WORK

TABLE OF CONTENTS

1	Network Services Overview	1
	1.1 Statement of Work Change Control	1
2	General Responsibilities	1
	2.1 Vendor Responsibilities.....	1
	2.1.1 Account Management.....	1
	2.1.2 Service Management Process.....	2
	2.1.3 Solution Support	2
	2.1.4 Compliance.....	3
3	Mode of Operation	3
	3.1 Phase 1: Network Design.....	3
	3.1.1 Vendor Responsibilities	3
	3.1.2 LEA Responsibilities	4
	3.2 Phase 2: Network Implementation and Transition.....	4
	3.2.1 Vendor Responsibilities	4
	3.2.2 LEA Responsibilities	4
	3.3 Phase 3: Ongoing Support.....	5
	3.3.1 Vendor Responsibilities	5
	3.4 The Vendor General Administration Services	5
	3.4.1 Vendor Responsibilities	5
	3.4.2 LEA Responsibilities	6
	3.4.3 Third-Party Vendor Management and Coordination	6
	3.4.4 General Performance Monitoring and Management.....	7
	3.4.5 Network Services – Managed Firewall Service.....	8
4	Internet Access Services	10
	4.1 Vendor Responsibilities.....	10

1 Network Services Overview

This Statement of Work documents the Services to be provided to TEA by the Vendor and sets forth the mutual understanding of the Parties regarding the roles, deliverables, and responsibilities of TEA and the Vendor, under the Master Services Agreement (the Agreement) entered into by the Parties as of the Effective Date.

The Vendor's solution consists of connecting LEA's current secure connection into the dedicated Vendor Environments supporting TEA. Bandwidth of 3mbps per the Vendor facility was calculated using a total end user count of 500,000.

The Service Level for the Vendor's Network Services is contained in Exhibit A-6 – Service Level Agreements.

The Vendor will meet agreed-on responsibilities as outlined in this Exhibit A-5 – Network Services SOW to provide timely production of the deliverables as well as meet Service Levels defined in Exhibit A-6. TEA will meet agreed-on responsibilities so that the Vendor can produce the agreed deliverables and Service Levels. The responsibilities set forth in Exhibit A-2 – Cross Functional Services apply to Network Services. 1.1 Glossary – General Terms

A glossary of definitions and explanations that apply to this Exhibit A-5 are provided in a separate document titled Exhibit A-1 – Definitions.

1.1 Statement of Work Change Control

Any change or modification to the Vendor's Services will be performed through the Change Control Procedures in Section 1.9 of the Agreement. If new or additional the Vendor services are required, such services may be provided pursuant to Section 1.3 of the Agreement and will be provided pursuant to the Terms and Conditions set forth herein and will then become part of the Vendor's Services. Any other changes or modifications to the Vendor's Services may be performed pursuant to the Change Control Procedures in Section 1.9 of the Agreement and would be provided pursuant to mutually agreed on Terms and Conditions. To the extent any such changes or modifications have not been agreed through the Change Control Procedures, the Vendor shall have no obligation to perform such modified services.

2 General Responsibilities

Network Services will establish, maintain, and support secure connectivity for each local education agency (LEA) as they migrate into the hosted Environments. The Vendor will provide a secure connection method for all LEAs. Each LEA will use their existing Internet connections to establish an secure session to the Vendor's-hosted server Environments using Vendor-supported Web browser. Network Services will maintain an Internet connection from each data center facility with sufficient bandwidth to support the network performance required to effectively develop, test, and run the SSIS for each migrated LEA.

2.1 Vendor Responsibilities

2.1.1 Account Management

- Act as a Single Point of Contact (SPOC) for management of the SMC and data center Network Services components supporting the hosted application

2.1.2 Service Management Process

- Develop a Network Migration Plan – as part of the overall Transition Plan for each LEA migrating into the Vendor-hosted Environment, the Vendor will operate and manage the secure connection authentication and policies regarding user authentication.
- Track and report plan progress, issues, and risks
- Make sure problem assessment and response is managed in accordance with the Vendor's standard Problem Management or Incident Management processes:
 - Perform fault isolation and Resolution to restore Vendor Services following a service disruption
 - Notify designated LEA ITS operations personnel and Vendor personnel when critical Network downtimes occur, using standard Vendor notification processes
- Provide all communications, documentation, and support in U.S. English
- Provide Authorized Users with technical support and advice regarding the proper use and functions of Network Services

2.1.3 Solution Support

- Conduct an initial design review meeting with TEA to present the Customer Network Design document for the designated Vendor site(s)
- Install, configure, and conduct testing on Network solution components located in the Vendor's facilities for each LEA migrating into a Vendor Environment
- Support mutually agreed-on telecommunication protocols
- Recommend an appropriate bandwidth for Internet connectivity to support performance requirements as LEAs migrate into each Vendor-hosted Environment
- Provide switching hardware and operating system software for all network components within the Vendor's data centers that host the systems
- Verify the switch configuration implementation plan with standard Vendor security audit procedures prior to the first production Go-Live LEA in each Environment.
- Conduct the Vendor service acceptance test according to the Vendor's standard template
- Maintain the equipment as deemed necessary by the Vendor to provide the Vendor's Services
- Refresh or replace the equipment as deemed necessary by the Vendor to provide the Vendor's Service.

- Remotely monitor the Vendor's platform twenty-four hours per day, seven days per week, 365 days a year (24x7x365) for availability and threshold exceptions
- Maintain the configuration files for devices receiving Vendor Services. Make the software configuration changes to the devices and control administrative access to those devices. Device configurations will be backed up in a network device configuration database. The database will be updated each time the configuration of a device is changed, and will retain the new configuration file, plus a limited volume of the previous versions of the file pursuant to the Vendor's standard practices. The Vendor will restore the appropriate file in the event of a hardware failure or other event that results in the corruption of the operating configuration file.
- Perform remote software configuration changes required to complete Install, Move, Add, and Change (IMAC) requests related to network equipment and services within the Vendor's data center

2.1.4 Compliance

- Adhere to LEA site access security and site policies that do not prevent the Vendor from meeting performance requirements of the contract
- Adhere to security and regulatory agreements as set forth in the Agreement

3 Mode of Operation

The following phases outline the processes used to deliver TEA's Network product or Services:

- Phase 1 – Network Design
- Phase 2 – Implementation and Transition
- Phase 3 – Ongoing Support

3.1 Phase 1: Network Design

The Network Design phase defines Network Architecture and associated details to meet LEA data communications requirements over the life of this contract. The design will include a proposed Network topology based on TEA's requirements, and a time-phased Implementation approach based on the migration plan of LEAs into a Vendor-hosted Environment.

During the Design Phase, the Network solution will be documented in the form of a Customer Network Design document that must be agreed to by TEA. This document will then be used to implement TEA's Network.

3.1.1 Vendor Responsibilities

- Document the Network solution in the form of a Customer Network Design document
- Use the Network Design document to implement the solution
- Update Network Design document as appropriate

3.1.2 LEA Responsibilities

- Maintain responsibility for appropriate local or remote connectivity, unless specified otherwise in the design, to support installation of any communications product/service/device.
- Comply with all obligations contained in any tariff, regulation, or any agreement with a third-party provider or applicable Local Exchange Carrier (LEC) that have an impact on the Environment in a Vendor data center
- Provide written approval of the Customer Network Design document to the Vendor and any updates based on changes to the LEA migration plan

3.2 Phase 2: Network Implementation and Transition

LEA requires network connections to the Vendor locations.

"Implementation" refers to the initial implementation of network equipment and processes to allow subsequent migration of LEAs into a Vendor-hosted Environment. This phase includes the designation of a project manager to assist the LEA with equipment procurement, if required, and management of Network Implementation activity.

"Transition" refers to the ongoing work effort required to successfully establish and test VPN connectivity between a Vendor site and a LEA migrating into a Vendor-hosted Environment.

3.2.1 Vendor Responsibilities

- Procure and provide all circuits and associated services that terminate in one of the Vendor's Network Operations Centers (NOCs) or data centers
- Oversee installation of the circuit(s) and associated equipment both in Implementation and as needed for each LEA Transition
- Perform functional testing of Internet circuits at the Vendor's facilities and the VPN connections provided to LEAs migrating into a Vendor-hosted Environment.
- Provide the Network infrastructure within the data center to support the SSIS application
- Provide the appropriate facility environmental conditions for circuits that terminate in a Vendor NOC or data center, to include floor space, power, electrical, air conditioning, uninterruptible power supply (UPS), diesel generator, and backup facilities
- Implement and support secure connections to the Network

3.2.2 LEA Responsibilities

- Order circuits and services that terminate in a Vendor NOC, SMC or data center
- Provide the Vendor with a LEA-specific contact for each LEA Transition into a Vendor-hosted Environment

- Participate in secure connection testing to ascertain successful connectivity with the Vendor's Environment

3.3 Phase 3: Ongoing Support

This phase covers the ongoing support for the management of the Vendor Network Services.

3.3.1 Vendor Responsibilities

- Provide a Level 1 trouble-tracking internal Network Service Desk for event logging
- Assist the Vendor's internal LEA delivery team with Network problem Resolution
- Act as the primary point of contact for the Vendor Services problem reporting

3.4 The Vendor General Administration Services

The Vendor General Administration Services coordinate, document, and maintain necessary Network administrative information required to effectively manage the LEA in-scope Network. The Vendor administers Network requirements and activities, such as processing Change Requests, Incident Management, and escalation procedures using the Vendor's Global Network Operations Center (GNOC).

3.4.1 Vendor Responsibilities

- Administer in-scope Network requirements and activities
- Review Service Request(s) and associated engineering requirements to establish expectations on requirements and delivery of Services
- Coordinate conference calls, acceptance plans, test criteria, and schedule service dates for in-scope Services
- Order, provision, and track Network equipment, data circuit, and consumables as specified in the bill of materials for the engineering work orders (EWO) or the infrastructure Service Request
- Document and maintain the following aspects of the Network Services for TEA:
 - Design criteria and standards
 - Escalation procedures
 - Service acceptance procedures
 - Topology documentation
- Maintain the following LEA and the Vendor supplier information pertaining to each LEA location that has or will soon migrate into a the Vendor-Hosted Environment:

- Site address and equipment room location
- Operational hours and days of the week
- Operational contacts and escalations: names, numbers, and e-mail addresses
- Site classification/business criticality

3.4.2 LEA Responsibilities

- Service Level Agreements (SLAs) with telecommunication providers, vendor contacts, and escalation procedures, such as electronic or automated methods and contact name and phone numbers, vendor maintenance contract numbers and identifiers, and contract terms and conditions
- Review and validate all transport vendor charges and dispute inaccuracies, when necessary
- Jointly establish service acceptance procedures
- Provide the Vendor with all appropriate Network documentation to support the Network

3.4.3 Third-Party Vendor Management and Coordination

Third-Party Vendor Management and Coordination Services coordinate third-party vendor activities using the Vendor's service delivery processes and procedures that take advantage of established communication and work channels with each third-party vendor.

3.4.3.1 Vendor Responsibilities

- Work cooperatively with third-party vendors and LEA staff to facilitate effective planning and design of the Network Services
- Provide and maintain plans and design for the following components:
 - Overall Network topology, consisting of the physical and logical layout of the Network
 - Network addressing schemes
 - Mutually agreed-on telecommunications protocols within the Network as required to support TEA's business and operational requirements
 - Network equipment
 - Network operational software
 - Transport systems
- Document and maintain the criteria and assumptions used to develop plans and designs for:

- Network bandwidth and/or volume assumptions and projections
- Expected Network performance and quality of service based on designs and plans, and minimum performance and quality of service expectations
- Expected Network Availability based on designs and plans for redundancy and minimum availability expectations
- Coordinate third-party vendor services and notify these suppliers, as required, to perform the specific services in accordance with the contracted service levels
- Monitor third-party vendor service delivery and performance
- Coordinate the execution of installs, moves, adds and changes (IMACs)
- Collaborate with third-party vendors to monitor, manage, and maintain software at agreed-on release levels

3.4.4 General Performance Monitoring and Management

General Performance Monitoring and Management Services provide remote administration of the Vendor-managed Network devices in the SMC and data centers through the Vendor's GNOC.

3.4.4.1 Vendor Responsibilities

- Provide a SPOC for Network-related issues
- Monitor and manage continuous end-to-end performance of the data center networks, consisting of monitoring the availability and performance of data Network resources, as follows:
 - Monitor the level and quality of service of the Network, including monitoring compliance with Service Levels
 - Monitor and manage the Network – including packet capture and analysis – for service degradation, consisting of detection, isolation, diagnosis, and correction of problems 24x7x365
 - Monitor physical and logical connections to the Network
 - Provide necessary monitoring, diagnostic and maintenance systems, and operational software to meet Network monitoring and management requirements
 - Support Network remote operations and monitoring comprised of remote diagnostics, remote administration, and remote problem Resolution, and, if necessary, travel to remote sites
 - Identify actual and potential Network bottlenecks and make recommendations to mitigate the bottlenecks
 - Perform necessary diagnostic routines

- Employ element management system tools to monitor events that exceed Network design thresholds and provide automated alarms and indications of Network problems when thresholds are exceeded
 - Monitor security information and events
- Perform a preliminary investigation of fault alerts to determine the cause of the fault
 - Open a ticket with the telecommunications provider for circuit-related faults
 - Direct third-party and vendor repair activity
 - Provide support to resolve complex or chronic problems requiring on-site expertise
 - Track issues through Resolution
 - Perform Root Cause Analysis
 - Notify LEA of the Resolution and close the ticket
- Notify LEA of the necessity of an unscheduled Service Interruption

3.4.4.2 LEA Responsibilities

- Notify the appropriate maintenance provider for Resolution of hardware or LAN cable-related problems

3.4.5 Network Services – Managed Firewall Service

Managed Firewall Services manage traffic flow and provide Network perimeter protection between networks. The Vendor will provide firewall appliances, rule-based administration, and software necessary to provide a secure network connection for LEA secure connection sessions to the Vendor's facilities as pertains to the hosted SSIS Environment.

Managed Firewall Services comprise:

- Provision of the Vendor's hardware and software
- Firewall administration
- System up/down monitoring of firewall availability, fault detection, and resolution
- Firewall configuration, backup, and restore
- Site-to-site Internet Protocol Security (IPSec) Virtual Private Network
 - Vendor-generated end-of-life technology Refresh for the Vendor-owned hardware

The Vendor will manage firewall services for Vendor-owned devices. Firewall administration for devices within LEAs is out of scope.

The following additional services are available to LEA on request and will be billed per incident at the time and materials (T&M) rates stated in the Exhibit A-7.2 LEA Pricing Scenarios:

- Rule-based changes
 - Firewall engineering

3.4.5.1 Vendor Responsibilities

- Provide administration of the firewall software policies and rules that govern the flow of traffic through the firewall
- Provide remote monitoring and fault detection for the firewall
- Configure and assist in testing the secure session(s) between the Vendor's managed firewall and the network device at the destination site(s) Refresh the technology as the Vendor deems necessary
 - Proactively, advise TEA of Refresh plans including rationale, timing, and impact
 - Perform technology refreshing on mutual agreement, at TEA expense, if TEA requests the Refresh for their specific business demands
 - Provide TEA-requested technology Refreshes pursuant to the Change Control process in Section 1.9 of the Agreement

3.4.5.2 LEA Responsibilities

- Assist in testing secure connection between LEA and the Vendor for access verification

3.4.5.2.1 Usage-Based the Vendor Services: Rule-Based Changes

The firewall rule-based Change Request turnaround time guidelines are shown in the following table. These are guidelines only and the actual turnaround time may vary.

Request Type	Request Definition
Regular	<p>Service requests for extending existing rules to cover a nominal number of additional Users or sources/destinations that take one hour or less to process</p> <p>Regular service requests are normally processed with a two-business day turnaround, based on workloads and size of change.</p>

Request Type	Request Definition
Expedited	TEA-requested simple expedited service requests are processed as soon as reasonably possible. The Vendor typically processes the change request within 24 hours, but the timing is based on workloads and size of the change.
Emergency	Emergency service requests are requested during non-Business hours, and the on-call administrative support personnel implements the rule change as soon as reasonably possible.

4 Internet Access Services

The Vendor uses Internet Access Services to manage Internet access, network monitoring of the Vendor's facilities, and management activities from its GNOC.

4.1 Vendor Responsibilities

- Configure, install, test, support, and maintain the Network and Network equipment used to access the Internet from Vendor sites
- Provide and manage Internet Access and Transport Facilities
- Manage routes and filtering as necessary
- Deliver Domain Naming System (DNS) services for domains required by the Vendor to manage the equipment
- Monitor the circuits and routers that comprise the Internet connectivity 24x7x365, identify faults, and dispatch personnel to correct faults, as necessary