

MASTER SERVICES AGREEMENT

between

TEXAS EDUCATION AGENCY

and

SKYWARD, INC.

JUNE 1, 2011

EXHIBIT A-2

CROSS-FUNCTIONAL SERVICES

STATEMENT OF WORK

TABLE OF CONTENTS

1	General Cross-Functional Services	1
1.1	Glossary – General Terms	1
1.2	Statement of Work Change Control	1
2	General Responsibilities	1
2.1	Vendor Responsibilities	2
2.1.1	Account Management	2
2.1.2	Service Management Process	2
2.1.3	Compliance	2
2.2	TEA Responsibilities	2
2.2.1	Account Management	2
2.2.2	Service Management Process	3
2.2.3	Compliance	3
2.3	Vendor Locations	3
2.3.1	Vendor Responsibilities	3
2.3.2	TEA Responsibilities	4
3	Cross-Functional Services	4
3.1	Service Desk – Level 2 Support	4
3.1.1	Vendor Responsibilities	4
3.2	Request Management	5
3.2.1	Vendor Responsibilities	5
3.3	Incident Management	6
3.3.1	Vendor Responsibilities	6
3.3.2	TEA Responsibilities	6
3.4	Change Management	7
3.4.1	Vendor Responsibilities	7
3.5	Problem Management	7
3.5.1	Vendor Responsibilities	8
3.5.2	TEA Responsibilities	8
3.6	Security Management Services	8
3.6.1	Security Administration	9
3.6.2	Server Virus Protection	10
3.6.3	Intrusion Detection Services – Host-Based	11
3.6.4	Incident Response – Emergency Response	11
3.7	Asset Management	12
3.7.1	Vendor Responsibilities	12
3.8	Disaster Recovery	12
3.8.1	Vendor Responsibilities	13
3.8.2	TEA Responsibilities	13

1 General Cross-Functional Services

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

The scope of Cross-Functional Services is as follows:

- Service Desk – Level 2 Support
- Request Management
- Incident Management
- Change Management
- Problem Management
- Security Management
- Asset Management
- Disaster Recovery

The Vendor will meet agreed-on responsibilities as outlined in this Exhibit A-2 – Cross-Functional Services SOW to provide timely production of the deliverables and Service Levels defined in Exhibit A-6. TEA will meet agreed-on responsibilities so that the Vendor can produce the identified deliverables and Service Levels. Each of the Parties shall be responsible and obligated to perform only those responsibilities stated in this document.

1.1 Glossary – General Terms

A glossary of definitions and explanations that apply to this Exhibit A-2 are provided in a separate document titled Exhibit A-1 – Definitions.

1.2 Statement of Work Change Control

Any change or modification to the Vendor 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 Services. Any other changes or modifications to the Vendor 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

2.1 Vendor Responsibilities

2.1.1 Account Management

- Provide one (1) resource as a primary point of contact to TEA. This contact will, in most cases, be the Skyward State Project Manager assigned to TEA.
- The Skyward State Project Manager will:
 - Oversee the provision of data center services under this contract
 - Work closely with TEA to define requirements for ongoing support, communicate status of the Environment, and escalate Problems or issues as necessary
 - Manage billing, invoicing, change order management, office/administrative support, staff management, account overall management, performance metrics, and other account management activities
- Anything that needs to be escalated will be escalated to the Skyward Account Executive (AE)

2.1.2 Service Management Process

- Participate in joint planning to integrate TEA and the Vendor current and future plans that will directly affect support of TEA's hosted Environments
- Use the Vendor standard processes to manage in-scope Cross-Functional services listed in Section 1 of this SOW
- Perform asset management and tracking of the Vendor-supported hardware and software
- Conduct Service Performance and Service Level reviews between TEA and the Vendor on a monthly basis, or as otherwise mutually agreed by the Parties
- Report on Service Level metrics as described in this SOW

2.1.3 Compliance

- Adhere to Vendor site access security and site policies
- Adhere to security and regulatory agreements as set forth in the Agreement

2.2 TEA Responsibilities

2.2.1 Account Management

- Provide a list of primary and backup contacts for ongoing interaction with the Vendor AE and Provide updates to the list as appropriate

- Provide and maintain lists of (a) authorized requests, (b) Problem or change submitters, and (c) change approvers for the Services performed by the Vendor
- Provide and maintain a written current escalation contact list for exception conditions
- Provide names of resources who are authorized to approve the Vendor system administration access to each TEA Environment hosted by the Vendor
- Provide business change forecasts that may affect the provisioning of Services provided by the Vendor, with reasonable lead time such that the Vendor can make the needed changes without compromising its ability to meet agreed Service Levels
- Make management decisions and provide information, authorizations, approvals, and acceptances on a timely basis so that the Vendor can deliver services properly, efficiently, and within time constraints
- Manage TEA third-party business partners, where the relationship is outside the scope of this Agreement, so that those business partners complete their responsibilities in a manner that does not negatively impact the Vendor performance
- Provide the Vendor with TEA's observed holidays

2.2.2 Service Management Process

- Appoint the Vendor as TEA's agent for management of third-party contracts and agreements, as appropriate, to enable the Vendor to perform its obligations under all SOWs

2.2.3 Compliance

- Assist the Vendor in understanding TEA security and regulatory policies as available and appropriate

2.3 Vendor Locations

The Vendor will create an infrastructure at one or more sites in Texas, designated as Skyward data centers, to support LEAs.

2.3.1 Vendor Responsibilities

2.3.1.1 Compliance

- Maintain appropriate physical security and access controls at the Vendor-designated data centers
- Secure systems located in the Skyward data center using the following physical security features:
 - Physical barriers and card access at all entrances
 - Card key authorization to access buildings and sensitive areas
 - Physical access granted to only authorized individuals with a business need for access

- Security camera monitoring of facilities
- Escort and monitor vendors or other non-Vendor individuals required to perform work on LEA's Environment, while on the Vendor premises
- Conduct a biannual SAS 70, Type II audit of all relevant Vendor data centers and report results to TEA

2.3.2 TEA Responsibilities

- Abide by the Vendor site security policies during all the Vendor site visits

3 Cross-Functional Services

This SOW is divided into the following cross-functional service areas:

- Service Desk – Level 2 Support
- Request Management
- Incident Management
- Change Management
- Problem Management
- Security Management
- Asset Management
- Disaster Recovery

3.1 Service Desk – Level 2 Support

The Vendor Level 2 Service Desk facilities will act as a single point of contact (SPOC) for LEAs' authorized User community and IT staff in their respective geographies to request the Vendor support for the Vendor-provided Services.

Levels 2 Service Desk hours of operation are 7:00 a.m.-6:00 p.m. CST Monday through Friday except on Skyward observed holidays. Service Desk support and monthly reports will be provided in English language only. The Service Desk will be supported by the Vendor's automated ticketing for management of customer requests.

To support LEAs, the Vendor Service Desk facilities will be located locally in the United States and act as the SPOC for LEAs' authorized User and IT community. Vendor support consists of addressing in-scope application and technical issues. The Vendor agents will take calls from LEAs' authorized submitters after LEA has performed troubleshooting steps and determined that the unresolved Problem is software- or Hosting-related.

3.1.1 Vendor Responsibilities

3.1.1.1 Account Management

- Provide a SPOC at the Level 2 Service Desk center supporting LEAs

3.1.1.2 Service Management Process

- Provide a toll-free phone number to each LEA who has opted out of ESC support
- Provide a toll-free number for Level 2 support between the ESC and the Vendor

3.1.1.3 Solution Support

- Receive calls from LEA's designated Authorized Users or IT support staff after LEA has performed Level 1 Service Desk steps
- Log customer requests in the Vendor corporate ticket system
- Log customer requests and assign priority based on Severity
- Dispatch calls electronically to designated secondary support organizations, as appropriate
- Initiate and follow escalation procedures as required to engage appropriate hosting and application management technical support teams, based on priority and urgency
- Provide notification regarding Severity 1 and security incidents to documented TEA business contacts and members of the Vendor support team.
- Skyward-direct-supported LEAs between 5,000 and 30,000 enrollment shall be allowed three (3) LEA personnel authorized to contact Skyward.
- For LEAs of 30,000 enrollment or greater, LEA personnel authorized to contact Skyward shall be no more than .01% of your student enrollment

3.2 Request Management

Request Management enables timely and effective delivery of requested services by applying a consistent approach for identification, routing, and Resolution of Requests that are not Incidents. Under the auspices of the Vendor Service Desk Service, Request Management provides intake, tracking, and escalation of hosting, application, and network-related system Problems, requests, and changes submitted by LEA- and ESC-authorized Super Users or IT support staff. The LEA or ESC Super Users or IT staff will serve as the first point of contact for LEA End Users and will attempt to provide needed assistance and resolve all Problems. If they cannot provide the needed assistance or resolve the Problem, they will contact the Vendor Level 2 Service Desk. The Service Desk will forward hosting, application, and network-related requests to the appropriate the Vendor service group for Resolution, based on priority and urgency.

3.2.1 Vendor Responsibilities

- Redirect Requests received from non-authorized submitters to the LEA-identified authorized submitters

- Log authorized LEA contacts requests in the Vendor corporate ticket system
- Assign priority based on business impact definitions established by TEA and the Vendor and documented in the Governance Manual
- Work with the LEA to understand the specific query
- Dispatch calls electronically to designated secondary support organizations
- Initiate escalation procedures as required to engage appropriate hosting, application management, and network technical support teams, based on priority and urgency
- Maintain escalation procedures as jointly defined by TEA and the Vendor and documented in the Governance Manual
- Track the query with the Problem Management ticketing system until resolved and closed

3.3 Incident Management

Incident Management initiates the break/fix activity, which focuses on repairing the system Outage, degradation, or other malfunction and restoring service as soon as possible to acceptable levels, as defined in the Governance Manual. When an Incident is reported, the Severity is identified based on various factors resolving or repairing something that isn't working correctly; the Incident classification is further defined in Exhibit A-6 – Service Level Agreements.

3.3.1 Vendor Responsibilities

- Redirect Incident requests received from non-authorized submitters to the LEA-identified authorized submitters
- For Incidents, create an Incident in the Vendor corporate ticket system:
 - Capture the following information: date and time the Incident was reported, Severity Level, the description, and other relevant information
 - Determine if a related existing Incident is already in the system; if so associate the new Incident with the existing one
- Perform diagnostics, identify the solution, and execute the action(s) required to resolve the Incident
- Complete the Incident documentation, consisting of actual start and end time of Incident; start Incident timer; activity taken to determine Resolution; corrective action taken; Resolution code; whether it is a temporary or permanent fix; and closure code
- Continue to track and monitor the progress of the Incident to Resolution

3.3.2 TEA Responsibilities

- Initiate and follow escalation procedures for any unresolved Incidents, as jointly defined by TEA and the Vendor and as documented in the Governance Manual, as required to engage appropriate TEA users or TEA third-party vendors to resolve the Incident

3.4 Change Management

The Change Management process as defined in Exhibit A-1 consists of the Vendor's change policies, procedures, and methods for implementing the State-sponsored SIS. The Change Management process facilitates and maintains an audit trail for hardware, system software, and environmental changes. The Change Management process results in changes to the computer environment being managed under the Vendor Change Management process, which consists of planning, documentation, scheduling, communication, approval, implementation, verification, and follow-up.

For clarification, the Vendor Change Management is not synonymous with the Vendor Change Control. Change Control, as defined in Section 1.9 of the Agreement, is the Vendor process by which a new Service or changes to an existing Service are managed.

3.4.1 Vendor Responsibilities

3.4.1.1 Service Management Process

- Provide Change Request notification requirements to LEA through release notes
- Execute the Vendor's standard Change Management process
- Receive a Change Request from the LEA
- Review the Change Request requirements for clarity and validity; facilitate modifications to the Request as appropriate
- Assign appropriate resources for the delivery of the Change Request
- Gather requirements, prepare a plan, assess risk and impact, and provide a cost estimate for the Change Request
- For Change Requests with costs associated, LEA signs off on the Tutorial, which provides a step-by-step description of the modification
- Engage and oversee execution of Change Request

3.5 Problem Management

- Problem Management focuses on determining the root cause and implementing a Resolution so that there is no recurrence. The Problem Management process tracks Problems that affect the TEA hosting, application management, and network environment. The process consists of Problem identification, recording, corrective action, root cause analysis, periodic trending for patterns of Problems, and management of trouble tickets. Problem Resolution is prioritized based on the severity of the Problem, using predefined Service Levels and Severity definitions agreed by TEA and the Vendor.

A complete, validated Request will be considered received once it has been logged into the Request Management system and assigned. A Request is not considered complete unless all information has been provided and appropriate authorizations and all prerequisite activities are complete.

3.5.1 Vendor Responsibilities

- Use the Vendor standard Problem Management process to manage Problems from identification through closure:
 - Accept Problem information from authorized submitters
 - Redirect Requests from non-authorized submitters to the TEA-identified authorized submitters
 - Create a Problem record, entering information obtained as a Service Request or trouble ticket into the Request Management system
 - Assess the Severity code and provide impact statements for Severity 1 Problems, describing an action plans to resolve the Problem
 - Initiate the Change Management process to apply a Resolution to a Problem, if required
 - Conduct a final review with the appropriate third-party supplier, if applicable, to make certain that the fault is eliminated from the computer environment
 - Close the Problem record according to established procedures
 - Conduct a technical review, as required, to identify the root cause of the Problem and determine if a permanent Resolution will require the Change Management process to be initiated
 - Provide support services in response to Requests for assistance related to the services
- Provide a Problem management summary review for each Severity Level describing the percentage of Problem tickets that were Resolved within the requisite period of time

3.5.2 TEA Responsibilities

- Review impact statements for Severity 1 Problems and provide feedback as needed

3.6 Security Management Services

Security Management Services protect the integrity, availability, and confidentiality of TEA information. Security Management Services focus at the infrastructure (such as network, server, or operating system) level and do not consist of application data security (for example, protecting specific rows of a database).

The Key Measures contained in Exhibit A-6 will adhere to the Vendor's Enterprise Security Policy and Standards. The Vendor will make this policy reasonably available to TEA personnel as requested by TEA, taking into consideration protection of the Vendor's intellectual property rights.

The Vendor exercises no control over the content of TEA's information passing through the network, which is made up of host computers, network hubs, and points of presence.

The following table lists in-scope Security Management Services.

Service	Description
Security Administration	The tools and processes to manage logical access to the Vendor-managed TEA information assets
Server Virus Protection	The antivirus software that is placed on each server to provide detection of and protection against viruses, worms, and other malicious code
Intrusion Detection Services (IDS) – Host Based	Detective controls using software tools and the process of monitoring, detecting, and identifying unauthorized activities on individual hosts
Incident Response – Emergency Response	Specialized technical and procedural support to provide guidance in defense against, containment of, and recovery from IT-based system incidents

3.6.1 Security Administration

Security Administration Services manage logical access to TEA information assets. These services consist of granting user logon IDs and access rights to system-level resources and maintaining server-level security parameters and security product options. This section describes the Security Administration Service activities and the associated TEA and the Vendor responsibilities. Security-related Service Levels and Service Performance measures are defined in [Exhibit A-6](#).

The Vendor will provide Security Administration to the extent possible based on granted access and role administration, available system capacity, installed security tool capabilities, and platform limitations.

3.6.1.1 Vendor Responsibilities

3.6.1.1.1 Service Management Process

- Secure resources (files/directories) according to the data owner specifications
- Assist authorized LEA contact with Problem determination and Resolution associated with system access, data access, and invalid access attempts, when requested by an authorized submitter
- Provide emergency support (at an additional cost) for access management for coverage beyond usual business hours based on potential impact, when requested by an authorized submitter
- Manage access to LEA data based on instructions provided by the Vendor
- Adjust and maintain operating system and security software parameters available in the specific operating system environment

- Provide processes and procedures to maintain operating system data protection options
- Coverage hours for Anti-Virus, Threat and Vulnerability, Intrusion Detection Services, and Emergency Incident Response are 24x7x365.
- Security Administration Services hours of coverage are as follows:
 - Monday through Friday, 8 a.m. to 5 p.m. Central Time (CT), excluding TEA observed holidays

3.6.1.1.2 Solution Support–Technical

- Configure operating systems at the setup of each server, make certain adequate security hardening rules are followed, establish Super User privileges and access rules, and establish other standard guidelines, based on the Vendor's Enterprise Security Policies and Standards (ESPS)

3.6.1.2 TEA Responsibilities

- Notify the Vendor upon the discovery of known unauthorized system access attempts or security violations

3.6.2 Server Virus Protection

Server Virus Protection provides antivirus software that is placed on each server to provide detection of, and protection against, viruses, worms, and other malicious code. The Vendor will update the antivirus software with current virus signatures and detection engines either automatically or by using electronic file distribution software. This service scans the server at the system level to detect malicious code.

3.6.2.1 Vendor Responsibilities

- Provide updated virus detection software and related signature files on servers to manage removal of malicious code according to industry standards
- Monitor supplier information and interface with suppliers to promptly receive the most up-to-date information on malicious code outbreaks and the appropriate software signature files to protect against the malicious code
- Provide support to administrators responsible for servers and systems to assist in the confirmation of malicious code, providing direction in the scanning for detection and removal
- Manage the process of communication and assist in mitigating a malware event
- Manage and provide the process and procedures for assigning a risk level to malicious code events, as well as factors to consider in assigning a risk level
- Assign a risk rating and associated method of action for malicious code based on the Vendor leveraged infrastructure environment

- Obtain and release signature files for testing and application into a TEA-dedicated environment
- Check servers on a regular basis for antivirus software to verify installation of the correct versions and levels and signature files

3.6.3 Intrusion Detection Services – Host-Based

Intrusion Detection Services (IDS) provide detective controls using software tools and the process of monitoring, detecting, and identifying unauthorized activities on individual hosts. This function enables system administrators to be immediately notified of unauthorized access attempts so action can be taken to limit exposure or potential loss. The Vendor's Computer Incident Response Team (CIRT) will respond to computer intrusion incidents.

3.6.3.1 Vendor Responsibilities

3.6.3.1.1 Service Management Process

- Install and maintain host-based intrusion detection software on servers to detect and generate real-time alerts for intrusion attempts using known methods for gaining unauthorized access
- Configure, test, and maintain rule sets for IDS software to provide real-time alerts when these established rule sets are broken
- Retain logs of generated alerts for future review, in accordance with the Vendor ESPS
- Establish and maintain monitoring consoles for the collection and analysis of traffic in a central repository
- Provide 24x7x365 monitoring of sensors for initial alert identification
- Conduct an analysis of alerts for validation of a potential security incident or breach
- Investigate alerts and take corrective action based on established Change Management processes
- Maintain a communication process for notification of suspected unauthorized intrusions or activities to administrators of attacked systems so action can be taken to block further intrusion
- Report to TEA, using pre-established processes, should an actual security breach incident occur

3.6.3.2 TEA Responsibilities

- Escalate immediately to the Vendor known unauthorized access to any server platform(s)

3.6.4 Incident Response – Emergency Response

Computer Incident Response – Emergency Response Service combines specialized technical and procedural support to provide guidance in defense against, containment of, and recovery from IT-based system incidents. The Vendor's CIRT will be engaged as a result of incidents identified through IDS, Virus Protection Services, or through other various avenues. An emergency incident consists of events of unauthorized access of resources, unauthorized modification of data, denial of service attacks against resources, or suspicion of these or similar activities. Computer Incident Response

Services is used to handle incidents affecting security appropriately and to minimize future damage to information, assets, and resources.

3.6.4.1 Vendor Responsibilities

3.6.4.1.1 Service Management Process

- Provide an Incident Report form to TEA for reporting incidents and verify that the necessary information is collected
- Review the Incident Report and determine appropriate action for containment and recovery
- Provide a report of Root Cause Analysis and recommendations for future avoidance to TEA
- Provide a summary of analysis and forensics activities to TEA, if requested
- Provide incident time line report to TEA, if requested
- Provide guidance and support in defense against future and similar, IT-based incidents
- Determine jointly with TEA the content, priority, and format of deliverables as a result of each incident response. In most cases, the Vendor will be able to supply an existing template, depending on the nature of the incident
- Maintain process and format for each incident response
- Provide an executive-level presentation to TEA, if requested
- Provide customized escalation and response plans to TEA for integration into TEA Change and Problem Management processes

3.7 Asset Management

The Asset Management process tracks IT-related business assets status and configuration throughout their life cycle.

3.7.1 Vendor Responsibilities

- Manage and control all business Asset activities within the Vendor-managed environments
- Establish and maintain data elements relevant to Asset Record profiles and verify business Asset data integrity through auditing activities
- Manage the life cycle of a business Asset until its end-of-life (EOL) disposition

3.8 Disaster Recovery

The Vendor's defined Disaster Recovery (DR) Services solution for TEA uses leveraged hosting services and standard recovery processes. The Vendor disaster recovery capability provides a recovery solution for the SSIS's critical applications, systems, and functions in the event of a Disaster as defined in Exhibit A-1.

The Vendor will support TEA's Environment in a designated Service Management Center (SMC) in the United States. Recovery site and hardware platforms for recovery of the Vendor-supported production Environment will be provided by a Vendor-managed subscription service at recovery facilities in the United States.

Additionally, the Vendor will provide application testing to validate the recovery of application data during the Disaster Recovery Plan (DRP) testing using the Vendor Disaster Recovery testing procedures agreed by TEA and as documented in the Governance Manual.

In the event of a Disaster, backup tapes will be sent from the off-site tape repository to recovery sites in the United States for recovery of the Vendor-managed operating system on an equivalent system platform. This service also provides a total of 32 contiguous-hours of annual testing to support the Disaster Recovery plan in each recovery facility.

3.8.1 Vendor Responsibilities

- With TEA, collaboratively develop a DRP for the Vendor-provided Services, including a plan for Disaster Recovery validation actions for the application
- Facilitate access to equivalent hardware at the selected recovery location if a Disaster occurs
- Provide resources to meet operating system recovery objectives for designated systems
- Secure backup media when transported offsite
- Test DRP once each year
 - Coordinate and schedule an equivalent leveraged environment for DRP test exercises
 - Provide the required resources to perform one annual DRP exercise of the hardware platform and operating system
 - Provide system support to TEA or TEA's application(s) provider for one annual DRP exercise of the application(s) and data
 - Schedule test activities for the Enterprise Application Management (EAM) Environment, perform application data recovery validation and document results
- Initiate a declaration of Disaster if a primary compute facility is rendered unusable
- Execute the agreed DRP in the event of a declared Disaster

3.8.2 TEA Responsibilities

- With the Vendor, collaboratively develop a DRP for the U.S provided Services

- Make appropriate user resources available during the Disaster Recovery testing to assist in the data accuracy validation
- Review validation results