

MASTER SERVICES AGREEMENT

between

TEXAS EDUCATION AGENCY

and

SKYWARD, INC.

JUNE 1, 2011

SCHEDULE 7.2

DATA SAFEGUARDS

The Vendor will provide the following data safeguards as part of hosting the SSIS server environment in one or more of the Vendor's data centers:

1 Electronically Controlled and Highly Restricted Access

The Vendor provides assurance that access to network equipment, computer equipment, storage media, and operations documentation is granted to authorized personnel only. Only authorized processing personnel have access to processing areas. Security cardkey readers protect all doors leading into the SMC. Once inside the SMC complex, access to other internal SMC areas requires cardkey access with increasing levels of security and access levels linked to required job function. The issuance of cardkeys for physical access to the SMC and other Vendor facilities is controlled through a request and approval process.

2 Biometric Controls

Access into restricted space within the Vendor's critical facilities that house client data incorporates biometric controls. No one is allowed to enter these locations without a valid card and biometric clearance. Positive biometric verification is tied to the access card. The bearer of the card must match the biometric presented in order to be granted access.

3 CCTV/Security System Integration

Protecting secured areas with badge readers or key locks and placing video cameras at all building entrances and exits enhances physical security. The Vendor's CCTV systems should be monitored 24x7, recorded, and back-up files are stored for 30 days. All security alarms are sent to the Security Control Room

4 Professional NOC Engineers 24x7

Professional NOC Engineers monitor Vendor data center buildings 24x7. Duties include emergency response, rounds, alarm acknowledgement and response, CCTV monitoring of the facility and property, incident detection and investigation, and reporting of incidents to management as appropriate for immediate resolution.

5 Visitor Escort

All visitors are required to be escorted within the building throughout the duration of their visit. The Vendor will provide client escorted access to locations where the Vendor provides services to the client for investigations and compliance reviews.

6 Audit Controls

The Vendor data centers must conduct a biannual, third-party SAS 70, Type II summary audit and report results to TEA, subject to TEA and its employees or agents having access to such information executing any confidentiality and nondisclosure agreement reasonably required by Vendor as a condition precedent to the disclosure of such information. TEA will review the audit findings and, if issues are found, make recommendations regarding the Vendor's service. Each audit includes a review of the Vendor's physical security processes and the execution of those processes.

Separated employees' access is removed immediately. The Vendor reviews access levels, including temporary access, at least quarterly to make certain that accesses are appropriate.

7 Fire and Smoke Detection and Suppression

The central monitoring station is equipped with environmental alarms for the facilities and communication devices for prompt, first-line response to any emergency.

8 Preventative Measures in Facilities

Within each data center, extensive environmental controls ranging from HVAC systems, generators, and multiple to redundant power supplies are installed to ensure that disaster recovery and business continuity plans are support both internally and for our clients. All equipment is regularly tested and inspected by the Vendor internally and by the maintenance provider.

9 Security Training

Hardware and software are essential to providing strong physical security, but the most important ingredient is personnel who understand the Vendor's security policies and standards and who are motivated to support and enforce them. All the Vendor employees are required to complete a security awareness training course annually.

10 Incident Reporting System

Security incidents are reported to the Vendor through in-house incident reporting systems monitored at all times by the Vendor personnel. Incidents involving unauthorized access to facilities, physical emergencies (such as fire) and all other security concerns that may affect a Vendor client are communicated via established Vendor channels and subsequently relayed to the client or as required within the terms of the contractual agreement.

See also Exhibit A-2 – Cross Functional Statement of Work for additional security services.