SERVICE PROVIDER SECURITY ASSESSMENT QUESTIONNAIRE

1. Describe your policies and procedures that ensure access to government information is limited to only those employees/Contractors who require access to perform your proposed services.

Elearning Experts maintains a formal security program materially in accordance with industry standards that is designated to: (i) ensure the security and integrity of the Customer Content; (ii) protect against threats or hazards to the security of integrity of Customer Content; and (iii) prevent unauthorized access to Customer Content.

Corporate office security measures include CCTV and a business security system.

Only authorized personnel have access to management networks and application networks. Remote access to networks and services is achieved via industry standard encryption protocols and virtual private networking (VPN).

Administrative and remote access is highly restricted and is approved by senior management using least-privilege principles. Granting and revocation of access can be accomplished in seconds by senior management.

Additionally, in application computing environments, each hosted site is executed in its own security context, with permissions and access separate from other sites. Such measures provide a layer of separation so that one site cannot access data from another site.

2. Describe your disaster recovery and business continuity plans.

Local backups are performed daily and stored externally to the production application servers. . These backups can be restored to a production learning site in the event of unexpected data loss.

Disaster recovery and business continuity includes backups of the components and configurations required for the restoration of the learning management system. The disaster recovery backups consist of:

- nightly copy of full backups
- 24 hour recovery time point (RTP)
- ability to restore backup to running server instances

In the event of a disaster necessitating the need for adisaster recovery, the latest available backup snapshot is restored to a running instance of the learning management system.

Continuity plans include redundancies at many levels, including utility power, generator, UPS,, network, server, power supply, virtual machine, and disk/storage redundancies.

3. What safeguards and practices do you have in place to vet employees and Contractors who have access to government information?

National, State, and County criminal, E-Verify, and educational background checks are performed on all employees and any personnel who have access to government information. Additionally, professional references are utilized to vet the quality and experience of such personnel. Background checks are repeated annually.

The security and confidentiality of our clients data is covered in New Hire Orientation, documented in a mandatory confidentiality agreement signed by all employees, contractors, and interns, and is continually reinforced by our internal security policies. Security is discussed with staff during project meetings and through company wide communications.

4. Describe and explain your security policies and procedures related to use of Contractors/sub -contractors.

Whenever contractors/sub-contractors are employed for a specific task, we create development environments for each to which only restricted access is granted on need to have basis. Such development environments are segregated in terms of network, firewall and vpn access from all other production virtual or physical servers. Random data is generally used to simulate production environment for testing purposes.

5. List any certifications that you have that demonstrate that adequate security controls are in place to properly store, manage and process government information (for example, ISO or SSAE certifications). Will these certifications be in place for the duration of the contract? Will you provide the state with most recent and future audit reports related to these certifications?

The hosting facility provided by Amazon Web Services (AWS) is SOC compliant with an AICPA Service Organization Control Report (formerly SAS 70), and has ISO 27001 certification.These compliance measures and certifications will be in place for the duration of the contract. To that end, the "*Description of Amazon Web Services System - Service Organization Controls 1 Report*" and the *AWS ISO 27001 Certification* documents can be provided upon request.

6. Describe the policies, procedures and practices you have in place to provide for the physical security of your data centers and other sites where government information will be hosted, accessed or maintained.

The computing cluster is located within Amazon Web Services' (AWS) ecosystem of services. Elearning Experts employees and contractors do not have any physical access to the computing cluster. Physical access to servers and server network equipment is controlled by existing AWS security, compliance, and policy frameworks.

7. Will government information be encrypted at rest? Will government information be encrypted when transmitted? Will government information be encrypted during data backups?

Production data is never at rest and hence does not lend itself to encryption at rest, although access to data is strictly controlled via aforementioned physical security protocols. All data in transmission between the data center and external hosts is encrypted with SSL. Local backups are not encrypted as they reside in a secure data center. Remote/off-site disaster recovery backups are block-level encrypted, meaning that when the disaster recovery host(s) are offline (at rest) the backup data is in an encrypted state. Further security enhancements are possible as part of a customized deployment.

8. Describe safeguards that are in place to prevent unauthorized use, reuse, distribution, transmission, manipulation, copying, modification, access or disclosure of government information.

Access to the servers where data resides is only allowed to senior staff and employees with immediate access need, and then only under direct supervision. Beyond that, access to backend environment is not allowed as a matter of policy to anyone be it lower level staff members or third party contractors. All maintenance and diagnostics are performed with the use of tools that interact with data in a controlled and secured manner. If it becomes necessary to interact with government data on the backend servers in a way other than by using approved tools, escalation to senior personnel or executive level staff would be required. All access to servers is performed through VPN by using encrypted keys for authentication.

9. What controls are in place to detect security breaches? Do you log transactions and network activity? How long do you maintain these audit logs?

Network monitoring tools and notifications exist to detect security breaches. Firewall logs and unapproved network activity are logged and kept for a minimum of 30 days.

The Totara and Moodle applications also support a number of security features, including ability to allow/deny specific IP addresses and blocks. Anti-virus scanning of files uploaded into the application is configured on the learning management system instance.

10. How will government information be managed after contract termination? Will government information provided to the Contractor be deleted or destroyed? When will this occur?

Contract termination policy includes removal of all data for a client from the application execution environment (including application, database, and storage servers) within a month of termination. Client data existing in local backup snapshots are purged after a 3 month period starting at the point of data removal from the application execution environment.

Remote/off-site disaster recovery backups are destroyed within one month of termination.

11. Describe your incident response policies and practices.

Incident Response Outline

- Discovery of incident
- Report of incident to CEO, COO, and CTO
- Investigation of incident
- Resolution of incident
- Documentation of incident

Security incidents affecting clients are reported to affected clients.

12. Identify any third party which will host or have access to government information.

No third party will host or have access to government information on any facility owned and operated by Elearning Experts.