pennsylvania
DEPARTMENT OF HUMAN SERVICES

Resource and Referral Tool RFP

A. System Monitoring / Audit Logging

1. Commonwealth will need access to application / administrative audit logs.

Supplier Response:

{insert response}

2. What level of verbosity will be logged for administrative and user activity, specifically around vital record modifications / creation / deletion?

Supplier Response:

{insert response}

3. Can the vendor provide a sample copy of the logs so the Commonwealth can see the level of detail that is captured?

Supplier Response:

{insert response}

4. How can Commonwealth staff gain access to specific log data for review?

Supplier Response:

{insert response}

5. Can reports be established within a customer administrative portal?

Supplier Response:

Figure 1: Report Menu

6. What logging tool does the vendor use? Splunk? Is there a dashboard capability to view unusual activities?

Supplier Response:

{insert response}

7. What protections does the vendor propose to protect inappropriate access to the database from internal users? Specifically, any vendor employees that may have administrative rights.

Supplier Response:

{insert response}

B. Hosting Locations and Impact of Outage

1. Confirm applicable FedRamp level (high or moderate level) is achieved. The FedRamp is required for the infrastructure and the application.

Supplier Response:

{insert response}

2. Confirm hosting locations are in the US (primary, backup, failover, etc.).

Supplier Response:

{insert response}

3. Confirm the system will be setup as High Availability using multiple regions or SLAs will apply to address business impact.

Supplier Response:

{insert response}

C. Incident Notification

1. The vendor must acknowledge they are responsible for a data breach.

Supplier Response:

{insert response}

2. Confirm vendor has agreed to data breach notification timeframes that are within the COPA ITPs – Note the Commonwealth policy is outlined in ITP-024; reporting the incident within thirty (30) minutes for critical/high or one (1) hour of detection for medium is required for Protected Information (ITP-SEC019)

Supplier Response:

{insert response}

D. Vulnerability Scanning

1. How often does the vendor perform vulnerability scanning (both authenticated and non-authenticated scans)?

Supplier Response:

{insert response}

2. The scan results need to be shared with Commonwealth staff.

Supplier Response:

{insert response}

E. User Authentication

1. Confirm the SaaS solution supports ADFS integration for user authentication.

Supplier Response:

{insert response}

2. Confirm the application will not require proxy bypass? This refers to Commonwealth users using the application. Since the application is cloud based the security team wants to make sure the access is set up properly instead of just bypassing all firewalls.

Supplier Response:

{insert response}

3. How will non-Commonwealth users access the application? Keystone Login/user is preferred – this requirement would need a change order to implement.

Supplier Response:

{insert response}

4. How are new users registered to use the application?

Supplier Response:

{insert response}

5. Does the application delegate administrative authority?

Supplier Response:

{insert response}