

### Data Security Template

If professional development offerings are delivered online, or sensitive data is collected or transferred as part of the professional development offering, the Offeror must complete this template. If any questions are not applicable, the Offeror must explain why.

1. A list of variables collected or transferred;

Insert response here.

2. Format(s) in which data will be provided;

Insert response here.

3. Methods used to ensure secure data transfer, including a method of protecting against unauthorized access to sensitive data;

Insert response here.

4. The number of data transfers and timeframe within which data can be made available to authorized personnel;

Insert response here.

5. A method of protecting against unauthorized access to sensitive data;

Please explain here.

6. Weekly backups with incremental daily backups and a 48-hour recovery from the loss of a data center including the loss of only 2 hours of data;

Please describe the disaster recovery plan here.

7. A suitable hosting environment;

NOT APPLICABLE

Please describe the environment including primary site location(s) and disaster recovery location(s), internet connectivity, power management and site security and describe the relationship between the primary site(s) and recovery site(s) and any industry certifications that these facilities have achieved (e.g. Tier III/IV, SAS70, SOC1, SOC2, etc.).

8. Data archival policies and any data purge policies;

Please describe here.

9. A process for handling and notification of a breach of non-public data;

Please describe here.

10. A process for the authorization of various roles associated with data access;

Please describe.

11. A policy for only allowing remote access using industry standard network security processes;

Please describe the methods used for remote access.

12. A process for ensuring security of data stored at the offeror's site as well as any server security policies;

Please describe and indicate whether the service has periodic and ongoing vulnerability and penetration testing.

13. A process for identifying and remediating software defects;

Please describe.

14. A process for incident management, change management, and release management;

Please describe.

**NOT APPLICABLE**

15. A process for how school divisions will get their data back in a form that can be used in the event of contract termination or expiration or if the a different service is desired;

Please describe.

16. Network-layer vulnerability scans conducted regularly;

Please describe.

17. Application-layer vulnerability scans conducted regularly;

Please describe.

18. Local operating system-layer vulnerability scans conducted regularly;

Please explain.

19. File integrity (host) and network intrusion detection (IDS) tools that are implemented to help facilitate timely detection, investigation by root cause analysis and response to incident;

Please explain.

20. Regular penetration testing, vulnerability management, and intrusion prevention;

Please explain.

21. Network devices that are located in secure facilities and under controlled circumstances (e.g. ID cards, entry logs);

Please explain.

22. A standard time frame regarding how quickly patches are applied from the time of supplier release;

Please explain.

23. Background checks on your firm's personnel with physical and/or administrative access to network devices, servers, applications and customer data;

Please explain.

24. Processes for authenticating callers and resetting access controls, as well as establishing and deleting accounts;

Please explain.

25. Protection against denial-of-service attack;

Please describe.

26. Technical measures and techniques for detection and timely response to network-based attacks such as distributed denial-of -service (DDoS) attack; and

Please explain.

27. A statement confirming that the offeror shall:

- a. Comply with Virginia's Information Technology Security Policy and Standards (<http://www.vita.virginia.gov/library/default.aspx?id=537#securityPSGs>);
- b. Comply with the Family Educational Rights and Privacy Act (FERPA);
- c. Meet cloud security requirements by a certifying body such as Fed-RAMP (<http://cloud.cio.gov/fedramp>), if applicable
- d. Include a product support program for users and administrators;
- e. Be Section 508 compliant ([http://www.vita.virginia.gov/uploadedfiles/vita\\_main\\_public/unmanaged/library/contingencyplanningguideline04\\_18\\_2007.pdf](http://www.vita.virginia.gov/uploadedfiles/vita_main_public/unmanaged/library/contingencyplanningguideline04_18_2007.pdf));
- f. Include a backup and recovery plan that is tested at least annually;
- g. Include an outage plan. Users shall be notified of anticipated and unanticipated outages;
- h. Adhere to the Student Privacy Pledge, located in [http://studentprivacypledge.org/?page\\_id=45](http://studentprivacypledge.org/?page_id=45);

**NOT APPLICABLE**

- i. Ensure that all data processed, stored and maintained by the offeror shall NOT leave the borders of the United States (including all online storage as well as data backups and archived data);
- j. Include a process that allows the State to audit the physical environment where a service is hosted;
- k. Include a process for securing non-public data at rest and non-public data in motion;
- l. Allow access to incident data for investigative purposes;
- m. Allow access to system security and audit logs;
- n. Patch software vulnerabilities routinely or automatically on all servers; and
- o. Encrypt data at motion and at rest.