External Agency Responsibility for Data Security Agreement

For the purpose of providing general statement of product function goes here, Product and Specific Vendor name goes here (hereafter called "the vendor"), may collect or be provided confidential data in a format inclusive of unique district wide student and staff identifiers and allowed to access and maintain – but not distribute - DistrictName' (DISTRICTNAME) student or staff data under the following conditions - which includes responsibility for keeping such data and the software systems involved with such data – secure.

The intent of this agreement is to clearly communicate to the vendor that the school district does not have sufficient knowledge of the specific software application design or functions, and the school district does not have available in-house expertise to adequately monitor that the software application and the data associated with this application has been properly secured and functioning.

In the case where the district provides the computer system environment for the application, the district will be responsible for back-ups of those system and data files identified by the vendor as necessary for system recovery. For hosted environments (computer system environment provided by the vendor) the vendor has the responsibility for backup of those systems and data files necessary for system recovery. It is the vendor's responsibility (in either environment) to confirm and monitor software system performance and integrity relating to data and system security. It is the vendor's responsibility to notify the school district when issues or problems arise.

Specifically:

1) The vendor is responsible for maintaining these data, including any copies or derivations - and the transmission of such data, in a secure environment and under controls to preclude access by anyone other than those specifically authorized for such access. The vendor, to the best of its ability, will ensure that access, dissemination, and maintenance of DISTRICT Schools' student or staff data (confidential or otherwise) is consistent with applicable rules, statutes, and "good sense" such as to respect the individual's right to privacy and due process.

   This involves the vendors attending to procedural, equipment and system requirements including but not restricted to: physical and electronic security of the data-resident servers and storage medium, safeguards and monitoring to restrict access to these data or systems by any unauthorized users, adequate controls and upkeep of rights to electronic files and folders, maintenance of secure server and client data locations and transmissions, and timely updates to data access and system user authorizations.

2) In the case where DISTRICTNAME provides the computer systems environment, the vendor is expected to provide specific guidelines and recommendations relating to the data required by the application, including specific recommendations relating to data transmission security, i.e. encryption, file transmission methodology, and file archiving/back-up/access or update logging.

3) In the event of a termination of this agreement, the vendor is responsible for destroying all copies or derivations of the data provided. In addition, the vendor will provide DISTRICTNAME a snap shot of current data at the time of termination and at least five days of daily backups in a media format agreeable to DISTRICTNAME.

4) The vendor is responsible for maintenance and monitoring of the software, specifically, it is expected that the vendor be actively and regularly monitoring the functioning of the software system; and if inappropriate intrusion or activity is detected, the vendor is expected to notify the school district immediately.

5) In the case where DISTRICTNAME provides the computer system environment, it is the district's responsibility to maintain system and database back-ups according to the written specifications provided by the vendor, and for reasonably timely application of security patches and fixes relating to the operating, communications, or database systems utilized by the software product whenever these are identified by the vendor and communicated to the school district. In a vendor hosted environment the vendor has the same responsibilities (database backups, application of security patches, OS fixes, etc.).

6) If the vendor fails to regularly monitor the software system functionality and integrity (i.e. monitoring as necessary to detect aberrant or system dysfunctions, such as denial of service attacks, virus, spyware or malware) and fails to also maintain critical security patches as relates to the software application, all unpaid fees and monies scheduled to be sent to the vendor will be frozen until appropriate system updates, recovery, or monitoring by the vendor is in evidence. The vendor will be noticed should this step be necessary.

7) It is the vendor's responsibility to test the software systems recovery from the prescribed back-up.

8) It is the vendor's responsibility to provide timely notification (typically immediate, via e-mail and telephone calls) to DISTRICT Schools in the event of any change or incident where there was a breach in the security such that these data were made available to parties or agencies outside those specified; and including any incident of unauthorized or inappropriate access to system files or data.

For further information regarding these procedures and guidelines, contact DISTRICTNAME Security Manager or IT Director at DISTRICT District Schools, Technology & Information Services.

I UNDERSTAND AND AGREE TO THE CONDITIONS SET FORTH IN THIS DOCUMENT.

_____ _____

SIGNATURE (Vendor Representative) **DATE**