DATA PRIVACY AND SECURITY POLICY

1. Network Security

Sourcewell Technology (“SWT”) will maintain network security that includes: network firewall provisioning, intrusion detection, and regular (three or more annually) third party vulnerability assessments. SWT will maintain network security that conforms to generally recognized industry standards ("Industry Standards", which are listed below in Section 10 below) and best practices.

2. Application Security

SWT will provide, maintain and support the software licensed to its customers and used internally, and subsequent updates, upgrades, and bug fixes as made available for such software so that it is and remains secure from those vulnerabilities as described in Industry Standards.

3. District Data Security

SWT will preserve the confidentiality, integrity and accessibility of educational data, including student data provided to it by school districts and similar customers (collectively, "District Data") with administrative, technical and physical measures that conform to Industry Standards and best practices. Maintenance of a secure processing environment includes, but is not limited to the timely application of patches, fixes and updates to operating systems and applications as provided by SWT or open source support.

4. District Data Storage

SWT will ensure that any and all District Data will be stored, processed, and maintained solely on designated target servers and that no District Data at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, unless that device or storage medium is in use as part of the SWT designated backup and recovery processes and encrypted in accordance with the provisions set forth below in Section 6.

5. District Data Transfer or Remote Access by District

SWT will ensure that any and all electronic transmission, exchange or transfer of system and application District Data with District and/or any other parties expressly designated in writing by District, e.g., vendors, shall take place via secure means (using HTTPS or SFTP or equivalent) and in accordance with the provisions set forth below in Section 8. SWT will provide District with a Data Transfer Agreement (or similar document) to sign before any such transfer occurs. In the event District

requests remote access to District Data via ODBC (open database connectivity), SWT will provide District with a Remote Access Agreement (or similar document) for signature by District and a similar agreement for signature by each individual using such access before remote access is available, subject to additional costs.

6. District Data Encryption

SWT will store all backup District Data as part of its designated backup and recovery processes in encrypted form, using a commercially supported encryption solution. Additionally, all District Data defined as personally identifiable information ("PII") under the FERPA (Family Educational Rights and Privacy Act) or as private data under the MGDPA (Minnesota Government Data Practices Act) stored on any portable or laptop computing device or any portable storage medium will be likewise encrypted. Encryption solutions will be deployed with no less than a 256-bit key for symmetric encryption and a 2048 (or larger) bit key length for asymmetric encryption.

7. District Data Ownership

SWT acknowledges and agrees that at no point in time is it the owner of District Data. Ownership rights are maintained by District, and District reserves the right to request the prompt return of any portion of District Data and/or all data files at any time for any reason whatsoever, subject to payment for time and materials at reasonable rates by District to SWT.

8. District Data Sharing

SWT will ensure that any and all District Data shall be used expressly and solely for the purposes enumerated in separate legal agreements. District Data shall not be distributed, repurposed, sold or shared across other applications, environments, or affiliates of SWT. Prior to any such distribution by SWT, it shall first obtain prior written permission from District.

9. De-Identified District Data

District understands and agrees that it hereby authorizes SWT to use District Data, including electronic student data, in a *de-identified format* as defined in FERPA, 34 C.F.R. §99.31(b)(1), for the following purposes and that SWT has no obligation to destroy or return such de-identified data upon termination: (1) to test Data for performance and compatibility with new software releases and upgrades; (2) to test Data in a new release against the existing environment; (3) to test for conversion; (4) to provide software support services to District in connection with their business relationship per separate agreements; and (5) for presentations or demonstrations to District and other school districts.

10. Security Breach Notification

If SWT becomes aware of a privacy incident or a security incident (each of which is defined below in this Section 10) regarding any District Data, SWT will report the event to the District and the District's Chief Technology Officer (or employee with similar title and responsibility) within five (5) business days, subject to any restrictions imposed by law enforcement authorities. The decision to notify and the actual notifications to the District's Data subjects affected by the security or privacy incident is the responsibility of the District. To the extent within the insurance coverage and limits of SWT's current insurance policy, subject to the provisions in Minn. Stat. § 466.06, if applicable, SWT shall indemnify, hold harmless and defend the District and its officers, and employees for and against any claims, damages, costs and expenses related to any privacy or security incident involving any District Data except to the extent caused by the District or a third party. SWT hereby agrees that District shall be an additional insured under its cyber liability insurance policy while SWT is providing Hosting Services to District. SWT and the District each have a duty to reasonably mitigate any harmful effects resulting from any privacy or security incident involving any District Data.

For purposes of this Section 10, "security incident" means the successful unauthorized access, use, disclosure, modification or destruction of data or interference with system operations in an information system. For purposes of this Section 10, "privacy incident" means violation of the MGDPA and/or federal privacy requirements in federal laws, rules and regulations. This includes, but is not limited to, improper or unauthorized use or disclosure of Not public data, improper or unauthorized access to or alteration of public data, and incidents in which the confidentiality of the District Data maintained by SWT has been breached. “Not public data” has the meaning set forth in the MGDPA, Minn. Stat. § 13.02, subdivision 8 (a).

11. Legal Requirements

SWT will comply with the MGDPA and the FERPA as it applies to all District Data collected, received, stored or maintained by SWT under separate legal agreements. The civil remedies of Minn. Stat. §13.08 apply to the release of District Data governed by the MGDPA by either SWT or District. If SWT receives a request to release any portion of District Data, SWT will promptly notify District.

12. Litigation Hold Request

Upon receipt of a written litigation hold request from District, SWT will assist the District to preserve all documents and data identified by District within the scope of the litigation hold. Such efforts will include the suspension of deletion, overwriting or similar destruction of the documentation and data identified by District.

13. District Audit Request

Upon receipt of a written request from District, and proposed Statement of Work, SWT will allow District to audit or review the security and privacy measures that are in place to ensure protection of District Data within a reasonable timeframe after the request, subject to the provisions in Minn. Stat. § 13.02, subd. 13 or Minn. Stat. § 13.37, subd. 1 (a).

14. District Data Handling Post Termination

Upon termination of separate legal agreements, and written request from the District, SWT will erase, destroy and render unrecoverable all District Data in conformance with Industry Standards. SWT will certify in writing that these actions have been completed within ninety (90) business days of such termination.

15. Industry Standards

Industry Standards include but are not limited to the current standards and benchmarks set forth and maintained by the following entities:

- Center for Internet Security - see http://www.cisecurity.org
- Payment Card Industry/Data Security Standards (PCI/DSS) - see http://www.pcisecuritystandards.org
- National Institute for Standards and Technology - see http://csrc.nist.gov
- Federal Information Security Management Act (FISMA) - see http://csrc.nist.gov e. ISO/IEC 27000-series - see http://www.iso27001security.com/
- Organization for the Advancement of Structured Information Standards (OASIS) - see http://www.oasis-open.org/The Open Web Application Security Project's (OWASP) "Top Ten Project" - see http://www.owasp.org; or
- The CWE/SANS Top 25 Programming Errors - see http://cwe.mitre.org/top25/ or http://www.sans.org/top25-programming-errors/

- "Clear" media sanitization according to the standards enumerated by the National Institute of Standards, Guidelines for Media Sanitization, SP800-88, Appendix A - see http://csrc.nist.gov/
- High Availability percentage calculation (i.e. percent uptime) - see http://en.wikipedia.org/wiki/High_availability