



## **HOSTING SERVICES AGREEMENT**

### **TIES (Technology and Information Educational Services)**

#### **1.0 Introduction**

This Hosting Services Agreement ("Hosting Agreement") sets forth the terms and conditions for TIES' provision of Hosting Services (defined below in Paragraph 3) to TIES' school district customer ("District") in connection with a separate End User Agreement for software specified in such agreement (the "Software"). District agrees to the terms and conditions in this Hosting Agreement by signing the End User Agreement.

#### **2.0 Hosting Services Fees**

District will pay TIES for Hosting Services as part of the Software license fee as specified the End User Agreement.

#### **3.0 Hosting Services**

While the End User Agreement (or a similar agreement) is in effect between the parties, and subject to payment of the fees per Paragraph 2, TIES will provide the hosting services described below (collectively, the "Hosting Services") to District:

##### **3.1 (a) Configuration Planning**

TIES will determine the specifications for and configuration of the computing resources (number and type of web server(s), process server(s), application database server(s), and load balancer(s) based on the processing and storage needs of the District using commercially reasonable methods and historical data from other similarly sized districts. This configuration planning is the basis for the System Hardware and Additional Software and Middleware required, and may change from time to time as system requirements change. TIES will continually monitor system performance and modify the configuration plan to maintain the service levels set forth in Section 4.1.

##### **3.1 (b) System Hardware**

TIES shall provide access to a digital information processing, transmission and storage system (the "System Hardware") enabling District to perform operations using the functionality of the Software and to make the information generated by and stored in the database(s) supported by the Software

available on demand by users. System Hardware, system software, load balancer, database software and database storage will be located at a TIES's managed data center.

### **3.1 (c) Additional Software and Middleware**

TIES will provide all Additional Software and Middleware software necessary for the Software, including installation and licensing of Window OS, Microsoft SQL or Oracle server, and SSL certificate(s).

### **3.1 (d) Configuration and Setup**

TIES will provide initial configuration including: operating system installation; database installation; patching the operating system and database; installing and configuring the Software and Additional Software and Middleware; creation and configuration of Production and Training environments and databases. The Training environment will be used for the purpose of testing upcoming updates or code changes, training end users in a non-production environment and other non-production uses mutually agreed upon by TIES and the District. Prior to the Software being implemented, TIES will provide final hardware configuration and application setup for setting proper District specific application parameters and District's organization specific information. TIES will be responsible for ongoing re-configuration of hardware and adjustments to application setup for additional module add-ons or changes to District infrastructure that require changes to the system configuration and application setup.

### **3.1 (d) (i) Restrictions**

District will have a limit as to the following configuration options in a hosted environment:

- Audit Trail: Audit detail will not be retained beyond ninety (90) days unless required by applicable law or regulation. Exceptions for Attendance and Grade Reporting Mark data will be retained for the current school year and purged prior to the start of the following school year.
- Process Queue: Process Queue results will be stored for a maximum of five (5) days.

### **3.1 (e) Software Updates**

TIES will provide support for the Software through installation of TIES provided modifications including remedial patches, hotfixes or security remediations addressing reported performance or functionality problems and "Upgrades", which are new releases or versions of the Software and Middleware software issued by the vendor as part of its software maintenance offering, typically indicated by a

change in the numeric identifier in the version number of the software. TIES will install patches and Upgrades in accordance with the Release Management provisions included in Paragraph 6 below in a commercially reasonable timeframe following its release of patches, hotfixes or Upgrades of the Software, or TIES's receipt of the patch or Upgrade from the Additional and Middleware software vendor. In addition to administering all updates to the Software, TIES is responsible for procuring and administering vendor-provided maintenance for any Middleware software supplied by TIES under this Hosting Agreement.

### **3.1 (f) Backup**

TIES shall create and maintain a backup plan whereby District Data (defined below in Section 7.1) is backed up to a TIES managed data center spanning multiple geographic locations. Backups are created at the end of each business day (EOD). An electronic backup is a backup of District Data for the purpose of off-site archival.

### **3.1 (g) Disaster Recovery**

TIES shall maintain a Data Protection capability to protect the District's Data in a physically separate Disaster Recovery location and provide a 48 hour RTO (Recovery Time Objective) and a 24-hour RPO (Recovery Point Objective).

## **3.2 Excluded Services**

All technological assets managed by District.

## **4.0 Availability of Hosting Services; Service Level Credits**

**4.1 Availability of Hosting Services.** Subject to the terms and conditions of this Hosting Agreement, TIES shall use its best commercial efforts to provide the Hosting Services an uptime of 99.9% throughout the term of this Hosting Agreement (not including any planned maintenance). TIES agrees to provide District with Service Level Credits pursuant to the provisions in Section 4.3 below for Hosting Services according to the formula included in the table below this Section 4.1, subject to the limitation that Service Level Credits provided by TIES will not exceed 50% of the monthly cost allocated to Hosting Services, which is \$2.00 per student. TIES makes no representation or warranty that Hosting Services will be available at all times and temporary disruptions shall not constitute a breach of this Agreement. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, THE RELIEF SET

FORTH IN SECTION 4.3 SHALL BE DISTRICT’S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO THE FAILURE OR NON-PERFORMANCE OF THE HOSTED SERVICES.

Actual Uptime	Experienced Unplanned Downtime per Month	Service Level Credit Available up to 50% limit
<99.9%-99.5%	Between 44 minutes and 3.6 hours	10%
<99.5%-99%	Between 3.6 hours and 7.2 hours	25%
<99%-90%	Between 7.2 hours and 72 hours	50%
<90%	Greater than 72 hours	100%

Reference: Section 8.15 (*Industry Standards, High Availability*)

**4.2 Scheduled Downtime.** TIES will perform service maintenance outside 8 A.M. to 5 P.M. Central Daylight Time (CDT) after providing District 72 hours' prior notice ("Scheduled Downtime").

**4.3 Service Level Credits.** In order to receive a Service Level Credit, District must first report any outage to TIES, and within fifteen (15) days of the event, submit a request for credit in writing to support@tiescloud.net. District must include the ticket number from the open trouble ticket with such request.

There shall be no Service Level Credits for outages:

- Caused directly or indirectly by the acts or omissions of District;
- Caused by the failure of equipment or systems provided by District or any third party not under the direction or control of TIES;
- Caused by a Force Majeure event as defined below in Section 4.4;
- During Scheduled Downtime as defined above in Section 4.2;

- Occurring with respect to a request or an order from District for a change in the Service; or
- Occurring while District is in breach of the Agreement.

**4.4 Force Majeure.** This term means delay or failure in performance to the extent such delay or failure is caused by fire, flood, explosion, accident, war, strike, embargo, governmental requirement, civil or military authority, Acts of God, labor interruption, delay in, or inability to obtain on reasonable terms and prices adequate power, telecommunications, transportation, raw materials, supplies, goods, equipment, or services or any other cause beyond TIES' reasonable control. Any such delay or failure shall suspend performance under this Hosting Agreement until the Force Majeure ceases.

## **5.0 Remote Hosting**

District will not be provided direct administrative access (remote desktop access) to any server within the TIES hosting environment. Any optional application interfaces requested by the District will be accomplished and/or loaded by TIES for an additional fee.

## **6.0 Release Management**

For all Production, Test and Training Environments, TIES will follow "Release Management Procedures" in completing changes in the products or product release levels in current use and in implementing application patches and Upgrades (collectively "Change Events"). These Release Management Procedures will in all cases provide for the following:

- (a) Advance notification to the District of the Change Event, its nature and expected timetable;
- (b) Written notice of application changes and modifications to screens or code;
- (c) Pre-testing of changes, including any modifications to screen or code in TIES or District non-Production environments; and
- (d) Coordination of the implementation of the Change Event with the District.

## **7.0 Proprietary Rights**

### **7.1 District Data**

District shall be solely responsible for providing, updating, uploading and maintaining the educational data stored on the hosting site and any and all files, pages, data, works, information and/or materials on, within, displayed, linked or transmitted to, from or through the Hosting Site, including without limitation, trade or service marks, images, photographs, illustrations, graphics, audio clips, video clips, e-mail or other messages, metatags, domain names, software and text (collectively, the "District

Data”). District Data shall also include any registered domain names provided by District or registered on behalf of District in connection with the Hosting Services.

## **7.2 Alterations**

Except as provided herein or by law, TIES may not alter, modify, change, remove or disable access to all or any portion of the hosting site or District Data stored on the System Hardware at the hosting site.

## **7.3 Ownership of District Data**

TIES acknowledges that the District Data is owned solely by the District. Following termination of this Hosting Agreement, if District requires TIES's assistance to extract and provide District Data to District, TIES will do so subject to District's agreement to pay TIES at its then current hourly rate. TIES further warrants that it shall not lease, sell, rent or otherwise disclose District Data to any third party without prior consent of the District.

## **8.0 DATA PRIVACY AND SECURITY**

### **8.1 Network Security**

TIES will maintain network security that includes: network firewall provisioning, intrusion detection, and regular (three or more annually) third party vulnerability assessments. TIES will maintain network security that conforms to generally recognized industry standards ("Industry Standards", which are listed in Section 8.15 below) and best practices that TIES applies to its own network.

### **8.2 Application Security**

TIES will provide, maintain and support the software and subsequent updates, upgrades, and bug fixes as made available for the Software so that such software is and remains secure from those vulnerabilities as described in Industry Standards.

### **8.3 District Data Security**

TIES will preserve the confidentiality, integrity and accessibility of District Data with administrative, technical and physical measures that conform to Industry Standards and best practices that TIES then applies to its own processing environment. 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 TIES or open source support.

### **8.4 District Data Storage**

TIES 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 TIES designated backup and recovery processes and encrypted in accordance with the provisions set forth below in Section 8.6.

### **8.5 District Data Transfer or Remote Access by District**

TIES 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 8.8. TIES 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), TIES 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.

### **8.6 District Data Encryption**

TIES 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.

### **8.7 District Data Ownership**

TIES 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 TIES.

## **8.8 District Data Sharing**

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

## **8.9 De-Identified District Data**

District understands and agrees that it hereby authorizes TIES 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 TIES 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.

## **8.10 Security Breach Notification**

If TIES becomes aware of a privacy incident or a security incident (each of which is defined below in this Section 8.10) regarding any District Data, TIES 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 TIES' current insurance policy, subject to the provisions in Minn. Stat. § 466.06, if applicable, TIES 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. TIES hereby agrees that District shall be an additional insured under its cyber liability insurance policy while TIES is providing Hosting Services to



District. TIES 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 8.10, "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 8.10, "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 TIES has been breached. "Not public data" has the meaning set forth in the MGDPA, Minn. Stat. § 13.02, subdivision 8 (a).

### **8.11 Legal Requirements**

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

### **8.12 Litigation Hold Request**

Upon receipt of a written litigation hold request from District, TIES 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.

### **8.13 District Audit Request**

Upon receipt of a written request from District, and proposed Statement of Work, TIES 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).

### **8.14 District Data Handling Post Termination**

Upon termination of the Hosting Agreement, and written request from the District, TIES will erase, destroy and render unrecoverable all District Data in conformance with Industry Standards. TIES will

certify in writing that these actions have been completed within ninety (90) business days of such termination.

### **8.15 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.

<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](http://en.wikipedia.org/wiki/High_availability)

## **Services and Support**

### **9.0 TIES's Responsibilities**

#### **9.1 (a) Telephone Assistance**

Telephone assistance during normal business hours (8am – 5pm CDT) will be provided to District in identifying and verifying the causes of suspected defects where reasonably available. This assistance includes the following activities:

- (a) Advice on work arounds for verified defects.

(b) Advice on completion and authorization for submission of the TIES Modification/Change Request form to report identified defects in the Software to TIES.

(c) Assistance related to questions on the use of the Software.

### **9.1 (b) Technical Support**

TIES will provide technical support as part of the Software license fee specified in the TIES End User Agreement. Such support includes but is not limited to, training, operations support, implementation services, conversion activity, project management, customization and programming, user assistance and consulting.

## **10.0 District's Responsibilities**

### **10.1 (a) Telephone Service**

District will ensure that only personnel properly trained in operation and usage of the Software will utilize telephone service and that sufficient and suitable computer time and personnel are made available to implement the corrections suggested by TIES.

### **10.1 (b) Online Support Service**

District will allow the use of online diagnostics on the Software if requested by TIES during problem diagnosis.

### **10.1 (c) Notification of Security Events**

District is responsible for notifying TIES of suspected District security events, system or network compromises, or other events that could impact the confidentiality, integrity or availability of the TIES managed applications or systems, any defects in the Software, reproducing the suspected defects in the unaltered Software; and, upon TIES's request and to the extent provided by law, providing additional data in machine-readable or interpreted form deemed necessary or desirable by TIES to reproduce the environment in which the defect occurred and installing defect correction and maintenance releases.

### **10.1 (d) Operations**

District is responsible for operations of the designated system including but not limited to:

1. Assuring proper designated system configuration, Software installation, verification, audit controls and operating methods.
2. Implementing proper procedures to assure security and accuracy of input and output, and restart and recovery in the event of a malfunction.
3. The District shall designate to TIES a person properly trained in the operation and usage of the Software to serve as District's primary contact with TIES for Hosting Services.

#### **10.1 (e) Payment of Fees**

District shall pay the Hosting Services fees (included in Software license fees) within thirty (30) days of receipt of each TIES invoice. District further agrees to pay a late payment charge at the rate of one and one half (1 1/2) percent per month on any unpaid amount for each calendar month (or fraction thereof) that such payment is late. Such fees are exclusive of out-of-pocket expenses for Hosting Services performed. Charges for actual and reasonable out-of-pocket expenses, if any, will be billed monthly as incurred.

### **11.0 Performance Of Services**

#### **11.1 (a) Subcontractors**

TIES reserves the right to assign personnel or to subcontract to third parties who are reasonably qualified to provide Hosting Services for the Software.

#### **11.1 (b) Timing**

While TIES will endeavor to provide services as promptly as reasonable under the circumstances, the timing of their rendition is subject to the availability of qualified personnel and requirements of other TIES districts. Because the time in which a defect correction or detour can be devised and tested cannot be accurately assessed in advance, all dates or times quoted for such services or their completion are estimates only and are subject to alteration.

### **12.0 Termination Upon Default**

TIES has the right but not the obligation to cancel the license granted per the TIES End User Agreement or by other provisions in this Hosting Agreement if District is in default in payment of any amount due TIES for a period of thirty (30) days or more. Either TIES or District may terminate this Agreement upon a material breach of any provision of this Hosting Agreement by the other party, subject to the

non-breaching party's right to cure the alleged breach within thirty (30) days of the date of written notice of default from the other party. Said written notice must set forth particulars of the alleged breach.