Frontline Technical Facts

Infrastructure Overview

Executive Summary

Frontline Education provides software solutions to the education market in the US and abroad. It is delivered as a web-based Software-as-a-Service (SaaS) solution to increase accessibility and reduce cost for our customers.

Built on a foundation of world-class, ISO 27001 compliant and SSAE 16 (SOC 2) certified data centers, Frontline Education's products and controls are designed to follow the security guidelines set forth in FIPS Publication 200 and the NIST Cybersecurity Framework, as well as to comply with pertinent Federal laws such as the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy and Protection Act (COPPA) and the Health Insurance Portability and Accountability Act (HIPAA). Extensive effort goes into ensuring that all customer data and personally identifiable information (PII) is safeguarded from unauthorized access or use at all times.

The Frontline Education infrastructure supports over 4.1 million users from more than 6,300 school districts. In a single day, we:

- Process over 325,000 absences and place over 3 million phone calls
- Receive over 18,000 candidate applications
- Process over 6.5 million Professional Development Requests and 200,000 evaluations per year
- Serve millions of pages to the Education Community around the world

Complete redundancy is provided at all levels of the infrastructure to ensure maximum up-time in the event of any emergency. This document provides details on how we provide cost-effective, secure and scalable software solutions to our global customer-base.

Global Presence

Frontline Education maintains data centers in five locations around the world: Four (4) in the United States and One (1) in Canada to support our Canadian customers. Each data center is ISO 27001 certified and is subject to an annual SSAE 16 Type II audit.

Our primary datacenters are in Philadelphia-PA, Dallas-TX, Cambridge-MA and Mississauga-CA. Our Phoenix-AZ data center serves as a "warm" disaster recovery site that is fully production ready.

For more information, please visit:

Philadelphia – http://www.sungardas.com/company/infrastructure/pages/philadelphia-pa-1500.aspx

Dallas – http://www.level3.com/~/media/files/factsheets/en_datactr_fs_datacenterlocations.pdf

Cambridge – http://www.level3.com/~/media/files/factsheets/en_datactr_fs_datacenterlocations.pdf

Phoenix – http://www.sungardas.com/company/infrastructure/pages/scottsdale-az.aspx

Mississauga – http://www.sungardas.com/company/infrastructure/pages/toronto-on-1800.aspx

Benefits of SaaS

- **Lower cost of entry:** You do not have to buy hardware, software or telecommunications infrastructure.
- **Lower Administrative Overhead:** We perform all system updates and upgrades so you can focus on using the software, not maintaining it.

- **Highly Accessible:** Because our software is delivered as a website, you and your users can work wherever you have an internet connection.
- **Highly Available:** We focus on the availability and performance of our systems to ensure that it is available when you need it.

Security

Physical Security. Our datacenters are monitored by data center personnel 24/7/365. Access to the data center is controlled via an access control list and all approved visitors must supply government issued photo ID and sign in prior to gaining access to the data center. All production areas within the data center are secured by electronic card key and/or biometric device.

Perimeter Security. Our datacenters are equipped with a fully redundant, multi-tier network architecture. This configuration provides multiple points of traffic inspection and ensures that systems of differing security levels are sufficiently segregated allowing only legitimate traffic to pass.

Intrusion Prevention. All Internet traffic is examined by an enterprise Intrusion Prevention System (IPS). This system is managed and monitored 24/7 by a team of highly skilled security experts who will react to any suspicious activity immediately.

Encryption. Frontline Education's website access is secured using 256-bit Secure Socket Layer (SSL) encryption. This ensures that all web interaction is secure and protected from unwanted observation. In addition to this, all confidential customer data is stored with a minimum 128-bit encryption to further safeguard customer data.

Access Control. The Frontline Education systems have been engineered with a "Build it right, then continuously monitor" mindset and employ administrative, physical and technical safeguards (such as those outlined in FIPS PUB 200) which are designed to secure customer data from unauthorized access, disclosure, alteration and use. Any systems that house confidential or sensitive customer information, and the policies which govern them, adhere to the limitations and regulations as prescribed by the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy and Protection Act (COPPA) and the Health Insurance Portability and Accountability Act (HIPAA):

- Access to customer data is only granted to authorized personnel on an approval basis (following the principle of least privilege) to ensure that authorized personnel only have as much access to customer data as is required to perform their specified duties.
- All personnel who have access to confidential or personally identifiable data receive regular training on the proper handling and treatment of such data prior to being granted access.
- Access Control Lists are routinely audited to ensure only authorized personnel have access to customer data.

Compliance. Frontline fully complies with the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA). HIPAA outlines stringent safeguards to protect personally identifiable information (PII) of individuals receiving health care, including students receiving special education aid at their school district. FERPA grants parents and students the right to provide written consent before the school district discloses PII from the student's education records, except to the extent that FERPA authorizes disclosure without consent. Frontline requires district provided disclosure in the event student PII is knowingly stored in our product(s). At this time, the Children's Online Privacy and Protection Act (COPPA) is not relevant to our product(s). In the future, if COPPA applies to any of our products, we will fully comply with all requirements and regulations.

Data Use. Any data collected through Frontline Education products will only be used for the purpose of delivering the subscribed services. We will never sell, rent, transfer, disclose, or distribute customer data without prior written consent. Aggregated data that does not contain personally identifiable information regarding Customer's users provided in connection with the Software and Services will be the Confidential

Information and property of Frontline. Upon termination of a contract with Frontline Education, the district can request a copy of all of their data held in Frontline Education products. Even after a contract termination the district will maintain all rights and privileges to the data stored in Frontline Education products and Frontline Education will continue to protect archived customer data with the same physical and logical security safeguards as an active customer.

High Availability and Redundancy

In any environment, the potential loss of a component or an entire sub-system is very real. The Frontline Education infrastructure has been designed to be elastic in order to handle traffic surges as well as maintain normal operations in the event of multiple hardware failures.

Our partnership with Sungard Availability Services complements our internally designed systems by providing additional protection in the event of the following scenarios:

- Loss of a Telco provider
- Loss of an Internet Service Provider
- DDoS Attack
- Extended regional power outages

The proprietary Frontline Education products have been developed as distributed systems allowing for individual sub-systems to be scaled as needed as demand increases.

Disaster Recovery

In the event of a more substantial emergency, such as an unrecoverable local issue or the loss of the entire data center due to some regional catastrophe, we are able to bring our systems back online, typically within one (1) hour, by performing a failover to our "warm" disaster recovery site over 2,000 miles away.

DATA INTEGRITY

- The Frontline Education products utilize an enterprise-level database management system with world-class fault-tolerance and backup mechanisms.
- The Frontline Education database relies on a fault-tolerant database cluster, which allows uninterrupted database access, even in cases of complete server failure.
- Database backups are taken daily and transferred to a secure location for storage and quick retrieval.
- Transactional backups are taken multiple times per hour and retained locally as well as at our "warm" disaster recovery site, to allow for a granular restore in the event of data-corruption or accidental deletion.
- All customer data are stored in no fewer than two distinct, secure locations to guarantee that the information will be available, even during the most severe conditions.
- Customer data that is found to be inaccurate may be reported to Frontline Education, at which point the data will be reviewed and updated at the customer's discretion.

System Monitoring

The Frontline Education production environment is monitored 24/7 by systems engineers utilizing a variety of automated monitoring and reporting tools.

AUTOMATED TOOLS

Self-healing systems. Automation is employed wherever possible to allow the system to take corrective measures as needed to resolve issues without human intervention.

Early alert systems ensure high responsiveness. Every aspect of the internal Frontline Education infrastructure is monitored at regular intervals and provides proactive notification to systems personnel so

that problems are addressed before there is an impact to system availability. In case of a system outage, systems personnel are immediately notified via telephone, pager and email to begin Incident Response.

External testing for system availability and performance. The Frontline Education web applications are monitored multiple times a minute to ensure users continually receive the highest level of application response. This monitoring is performed using enterprise-grade web performance tools which simulate user activity from 15+ geographic locations across the United States and Canada.

Error notification built into application components. Each critical proprietary Frontline Education application has been designed to notify the Frontline Education systems personnel when problems occur. This ensures that any application issues are immediately detected and resolved.

ON-CALL PERSONNEL

Frontline Education personnel on standby 24/7/365. Frontline Education systems personnel are available at all times to respond to any issue that could cause system unavailability. Each Frontline Education engineer has adequate access to necessary systems to triage, troubleshoot and resolve system issues.

About Frontline Education

Frontline Education is a privately-owned corporation that develops human capital management and student data management solutions. Founded in 1998, the company provides a suite of software solutions for K-12 school districts. With a dedicated staff that adheres to strong moral and ethical principles, Frontline Education recognizes the importance of customer satisfaction and operates with high standards of achievement.

1400 Atwater Drive

Malvern, PA 19355

Phone: 610.727.0370

Fax: 610.363.3710

Learn more about Frontline's commitment to security at www.FrontlineEducation.com/SecurityProtocol.