Contract Addendum

Protection of Student, Teacher, and Principal Data

1. Applicability of this Addendum

The Jefferson, Lewis, Hamilton, Herkimer, Oneida BOCES ("BOCES"), an educational agency, and CompanyMileage.com, LLC ("Vendor") are parties to a contract dated 09/04/24 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, SureMileage, SureExpense & SureMobile [name of product(s) covered by contract] ("Product"). BOCES' use of the Product results in Vendor receiving student, teacher, or principal personally identifiable information as defined in federal and state statute, including New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2. Definitions

2.1 "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes "Protected Information" covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.

2.2 "This Contract" means the underlying contract as modified by this Addendum.

2.3 "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by Vendor from BOCES or is created by the Vendor's product or service in the course of being used by BOCES. "Protected Information", as applied to Teacher or Principal Data means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

2.4 "Breach" means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.

3. **Vendor Status**

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

4. **Confidentiality of Protected Information**

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the BOCES Policies on Data Security and Privacy and the Parent's Bill of Rights for Data Privacy and Security, copies of which are Attachment B to this Addendum.

5. **Vendor Employee Training**

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

6. **No Use of Protected Information for Commercial or Marketing Purposes**

Vendor warrants that Protected Information received by Vendor from BOCES or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; shall not be used by Vendor or its Assignees to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students.

7. **Ownership and Location of Protected Information**

7.1 Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with BOCES. Vendor shall acquire no ownership interest in education records or Protected Information.

7.2 BOCES shall have access to the BOCES' Protected Information at all times through the term of this Contract. BOCES shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.

7.3 Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by BOCES or its authorized users, or performing any other data analytics other than those required to provide the Product to BOCES. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to BOCES upon request.

7.4 All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada. All helpdesk, online, and support services which access any Protected Information must be performed from within CONUS or Canada.

8. **Purpose for Sharing Protected Information**

The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to BOCES.

9. **Downstream Protections**

Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by another entity, that entity shall be deemed to be an "Assignee" of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Information with such entities if those entities are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.

10. **Protected Information and Contract Termination**

10.1 The expiration date of this Contract is defined by the underlying contract.

10.2 Upon expiration of this Contract without a successor agreement in place, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES.

10.3 Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities.

10.4 Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

10.5 To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10.6 Upon request, Vendor and/or its subcontractors or assignees will provide a certification to BOCES from an appropriate officer that the requirements of this paragraph have been satisfied in full.

11. **Data Subject Request to Amend Protected Information**

11.1 In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the BOCES for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

11.2 Vendor will cooperate with BOCES in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

12. **Vendor Data Security and Privacy Plan**

12.1 Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.

12.2 Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

a. aligns with the NIST Cybersecurity Framework 1.0;

b. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

c. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract,

consistent with the BOCES data security and privacy policy (Attachment B);

d. specifies the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;

e. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

f. specifies how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

g. specifies if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

h. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify BOCES; and

i. describes whether, how and when data will be returned to BOCES, transitioned to a successor contractor, at BOCES' option and direction, deleted or destroyed by the Vendor when the contract is terminated or expires.

13. Additional Vendor Responsibilities

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations may subject the vendor to a monetary civil penalty and shall be a breach of this Contract:

13.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

13.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;

13.3 Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the BOCES unless (1) Vendor has the prior

written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the

disclosure is provided to BOCES no less than three (3) business day prior to disclosure, unless such notice is expressly prohibited by the statute or court order;

13.4 Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

13.5 Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

13.6 Vendor will notify the BOCES of any breach of security resulting in an unauthorized release of student data by the Vendor or its Assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of the breach; and

13.7 Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse BOCES for the full cost incurred by BOCES to send notifications required by Education Law Section 2-d.

Dated: 09/04/2024

Michele A. Carpenter
_____

For the Jefferson-Lewis BOCES

_____

For the Vendor

JEFFERSON • LEWIS • HAMILTON • HERKIMER • ONEIDA
BOARD OF COOPERATIVE EDUCATIONAL SERVICES

Attachment A - Supplemental Information about this Contract

CONTRACTOR: CompanyMileage.com LLC

PRODUCT: SureMileage, SureExpense (optional), SureMobile

PURPOSE: Manage mileage & expense reimbursement

DETAILS: The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to BOCES. The product or services are used to provide [e.g., mathematics instruction in Grades 1 and 2].

SUBCONTRACTOR DETAILS: Vendor represents that it will only share Protected Information with subcontractors if those subcontractors are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.

DATA DESTRUCTION

INFORMATION The agreement expires | Month to Month contract

Upon expiration of this Contract without a successor agreement in place, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES. Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

DATA ACCURACY

INFORMATION: In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law

Dated: 09/04/2024

Michele A. Carpenter
_____

For the Jefferson-Lewis BOCES

_____

For the Vendor

Attachment B - Parents' Bill of Rights for Data Privacy and Security and BOCES Data Security Policy

Pursuant to New York State Education Law §2-d, parents, legal guardians and persons in parental relation to a student, as well as eligible students, defined as those students who are eighteen years or older, are entitled to certain rights with regard to their child's personally identifiable information (PII), as defined by Education Law §2-d. Jefferson-Lewis BOCES Policy 6001 contains a Plain-English summary of such rights. Vendor specifically acknowledges receipt of Parents' Bill of Rights for Data Privacy and Security and BOCES Data Security Policy, which are attached hereto, and understands its legal obligations as provided therein.

https://www.boces.com/page/dataprivacy

Dated: 09/04/2024

Michele A. Carpenter
_____

For the Jefferson-Lewis BOCES

_____

For the Vendor

Attachment C – Vendor's Data Security and Privacy Plan

The BOCES Parents Bill of Rights for Data Privacy Security, receipt of which is acknowledged as Attachment B to this Addendum, is incorporated into and made a part of this Data Security and Privacy Plan.

[INSERT LINKS OR TEXT, AS PROVIDED BY THE VENDOR]

See following Internal Controls Summary

Dated: 09/04/2024

Michele A. Carpenter
For the Jefferson-Lewis BOCES

For the Vendor

Internal Controls Summary

CompanyMileage.com
MANAGING COST ONE MILE AT A TIME

Revised April 2023

Security Policies and Procedures

CompanyMileage has the following security procedures and policies.

- Access Control Policy
- Password Policy
- Change Management Policy
- SDLC Policy
- Backup and Recovery Policy
- Incident Management Policy

Data Encryption

- Split knowledge, dual-control passwords
- Table-level encryption
- Password rotation management
- Log file encryption
- Privileged user (root) protection
- Compliance with PCI DSS, HIPAA, HITECH, FISMA and other regulatory guidelines for encryption of data at rest
- PCI certification
- Secure offsite key management

Secure Facilities and Equipment

- Primary servers are hosted and managed by Rackspace's data centers with 24/7 management and monitoring
- Synchronized servers are hosted by Amazon Web Services data centers with 24/7 management and monitoring
- Data centers are SSAE 16/ISAE 320 certified
- Daily backups
- Secure servers running RedHat Linux are maintained and serviced daily with any security patches
- Firewalls are in place to prevent unauthorized access to the system
- 256 bit encryption SSL

SureMileage and SureExpense System | Summary of System and Organization Controls

Internal Control Framework

- Policies and Procedures to address critical, financial and operational processes have been implemented.
- Control Environment
- Risk Assessment
- Monitoring Activities
- Information & Communication
- Control Activities
    - ◊ Logical Access
    - ◊ Physical Security
    - ◊ System Operations
    - ◊ Change Management and Software Development Life Cycle
    - ◊ Identification of Features and Functions
    - ◊ Development
    - ◊ Source Code Review
    - ◊ System Integration Testing
    - ◊ Management Sign-Off
    - ◊ Deployment

Privacy Policies

- Client address books can be segregated by individual user, department or division
- Client names can be suppressed on physical reports generated by users
- CompanyMileage will not share client data with any third parties without written authorization from client
- CompanyMileage data systems are securely stored and accessible only by authorized company officials

Transaction Processing

- Client Setup and Account Maintenance checklists and standard procedures are in place.

Infrastructure Overview