IRAN DIVESTMENT ACT OF 2012 CERTIFICATION

As a result of the Iran Divestment Act of 2012 (Act), Chapter 1 of the 2012 Laws of New York, added new provisions to the State Finance Law (SFL), §165-a and General Municipal Law (GML) §103-g effective April 12, 2012. Under the Act, the Commissioner of the Office of General Services (OGS) will be developing a list (prohibited entities list) of "persons" who are engaged in "investment activities in Iran" (both are defined terms in the law). Pursuant to SFL § 165-a(3)(b) and GML §103-g, the initial list is expected to be issued no later than 120 days after the Act's effective date, at which time it will be posted on the OGS website.

By submitting a response to this solicitation or by assuming the responsibility of a Contract awarded hereunder, Vendor (or any assignee) certifies that once the prohibited entities list is posted on the OGS website, it will not utilize on such Contract any subcontractor that is identified on the prohibited entities list.

Additionally, Vendor is advised that once the list is posted on the OGS website, any Vendor seeking to enter into, renew or extend a Contract or assume the responsibility of a Contract awarded in response to the solicitation, must certify at the time the Contract is bid upon or a proposal submitted, or the contract is renewed, extended or assigned that it is not included on the prohibited entities list.

During the term of the Contract, should BOCES receive information that a person is in violation of the above-referenced certification, BOCES will offer the person an opportunity to respond. If the person fails to demonstrate that it has ceased its engagement in the investment which is in violation of the Act within 90 days after the determination of such violation, then BOCES shall take such action as may be appropriate including, but not limited to, imposing sanctions, seeking compliance, recovering damages, or declaring the Vendor in default.

BOCES reserves the right to reject any bid, proposal or request for assignment for an entity that appears on the prohibited entities list prior to the award of a contract, and to pursue a responsibility review with respect to any entity that is awarded a contract and ~~appears on~~ the prohibited entities list after contract award.

Signature: Mercedes Burgos

Print Name: Mercedes Burgos

Title: President

Company Name: MML Software LTD d/b/a FINANCE MANAGER

Date: 5/14/24

PARENT'S BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Ulster BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law S2-d, Ulster BOCES wishes to inform the community of the following:

1 . A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record.

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by the State is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to:

Ulster BOCES
175 Route 32 North
New Paltz, New York 12561

or

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234

Complaints may also be directed to the
Chief Privacy Officer (CPO) via e-mail at
CPO@mail. nysed.gov

6. The District Superintendent shall develop regulations to ensure compliance with all state and federal laws and regulations regarding the protection and security of student data as well as teacher or principal data.

Supplemental Information Reaarding Third Pady Contractors

In the course of complying with its obligations under the law and providing educational services, Ulster BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, thirdparty contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law.

Each contract Ulster BOCES enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include the following information:

1 . The exclusive purposes for which the student data or teacher or principal data will be used by third party contractor;

2. How the third party contractor will ensure that the subcontractors, persons or entities with whom the third party contractor will disclose the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

3. The duration of the contract, including when the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

4. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected;

5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated.

6. Address how the data will be protected using encryption while in motion and at rest.

Signature: ________________

Print Name: Mercedes Burgos

Title: President

Company Name: MML Software LTD d/b/a Finance Manager

Date: 5/14/24

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and __MML Software LTD d/b/a Finance Manager____________________ (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Ulster County BOCES ("BOCES") and Contractor to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that Ulster County BOCES' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"Protected Data" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by Ulster County BOCES. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of Ulster County BOCES as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of Ulster County BOCES 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.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with Ulster County BOCES policy(ies) on data security and privacy. Contractor shall promptly reimburse Ulster County BOCES for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of Ulster County BOCES' data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of Ulster County BOCES' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;
3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;
6. Specifies whether Protected Data will be returned to Ulster County BOCES, transitioned to a successor contractor, at Ulster County BOCES' option and direction, deleted or destroyed by the Contractor when the contract is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);
2. Comply with the data security and privacy policy of Ulster County BOCES; Education Law § 2-d; and Part 121;
3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;
5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or
b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, BOCES board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;
7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and
8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of Ulster County BOCES' Parent Bill of Rights.

NAME OF PROVIDER: MML SOFTWARE LTD d/b/a FINANCE
MANAGER____________________________

BY: Mercedes Burges_____ DATE: __5/14/2024___________
President

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

FINANCE MANAGER

DATA SECURITY AND PRIVACY PLAN

1. **Purpose.** The purpose of this Data Security and Privacy Plan is to define Finance Manager's security and privacy practices related to processing an Educational Agency's ("Customer") Personally Identifiable Information contained in (i) Student Data and (ii) Teacher or Principal Data (collectively, "Protected Data") in compliance with the requirements of New York Education Law 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d").

2. **Definitions**. Unless otherwise specified herein, all capitalized terms will have the meaning given to them in Section 2-d.

3. **Plan.**

    a. **General.** When processing Protected Data, Finance Manager:

        i. Follows policies and procedures compliant with (i) relevant state, federal, and local data security and privacy requirements, (ii) relevant contractual requirements between Finance Manager and the Customer; and (iii) the Customer's data security and privacy policy;

        ii. Implements commercially reasonable administrative, technical, operational, and physical safeguards and practices to protect the security of Protected Data in accordance with Section 2-d (*see* Section (b) below);

        iii. Follows policies compliant with the Customer Parents' Bill of Rights and Parents' Bill of Rights Supplemental Information;

        iv. Annually trains its officers and employees who have access to Protected Data on applicable federal and state laws governing confidentiality of Protected Data; and

        v. In the event any vendors are engaged to process Protected Data, manages relationships with vendors and contracts with vendors to protect the security of Protected Data.

    b. **Safeguards**. Finance Manager maintains reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its possession, including the following:

        i. Finance Manager identifies reasonably foreseeable internal and external risks relevant to its administrative, technical, operational, and physical safeguards;

        ii. Finance Manager regularly assesses the sufficiency of safeguards in place to address identified risks;

        iii. Finance Manager adjusts its security program in light of business changes or new circumstances;

        iv. Finance Manager regularly tests and monitor the effectiveness of key controls, systems, and procedures; and

v. Finance Manager follows written policies to protect against the unauthorized access to or use of Protected Data.

c. **Training.** Finance Manager trains personnel with access to Protected Data on the federal and state laws governing confidentiality of such data prior to receiving access and annually thereafter.

d. **Vendors**. In the event that Finance Manager engages any vendor to process Protected Data, it will (i) conduct due diligence and appropriate risk assessments before first allowing the vendor to access Protected Data, (ii) perform appropriate oversight of such vendor throughout the engagement with the vendor; and (iii) require its vendors to agree to contractual terms to protect Protected Data, including by obligating the vendor to abide by all applicable data protection and security requirements for Protected Data.

4. **Data Security and Privacy Incidents**. Finance Manager will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, by following an Incident Response Plan (IRP) for identifying and responding to incidents, breaches, and unauthorized disclosures. Finance Manager provides notice of Breaches to Educational Agencies in accordance with its Incident Response Plan and applicable laws.

5. **Return and/or Destruction of Protected Data**. Finance Manager will implement procedures for the return, transition, deletion and/or destruction of Protected Data as follows: Finance Manager deletes all Protected Data within ninety (90) days of expiration or termination of the agreement with Customer. For clarity, the Customer, and not Finance Manager, stores and maintains all production copies of Protected Data.

Data Security and Privacy Plan

Version 1.0

Table of Contents

1.0 Purpose

The purpose of this Data Security and Privacy Plan is to document **FINANCE MANAGER** commitment and approach to protecting Confidential Information (as defined in Section 2.0 of this plan), and how it will handle any incidents where there is a breach or unintended disclosure of Confidential Information or a System (as defined in Section 2.0 of this plan) that supports it.

2.0 Terminology

Application – means **FINANCE MANAGER** software that performs a user-facing function, such as a web application.

Confidential Information or Data – means any personally identifiable information related to students, student families/guardians, local education agency (LEA) employees, agents and/or volunteers obtained by or furnished to the Vendor; all findings, analysis, data, reports or other information learned or developed and based thereon, whether in oral, written, graphic, or machine-readable form; and all information marked "confidential" by the LEA. Confidential Information includes, but is not limited to, names, addresses, contact information, school or school attended, school district, grades or other reviews, credits, scores, analysis or evaluations, records, correspondence, activities or associations, financial information, social security numbers or other identifying numbers or codes, date of birth or age, gender, religion, sexual preference, national origin, socio-economic status (including free/reduced lunch status), race, ethnicity, special education status, or English Language Learner status, and any other information that constitutes "personally identifiable information" as defined in or pursuant to the Family Educational Rights and Privacy Act (20 U.S.C. 1232g and 34 C.F.R. Part 99) (collectively, "FERPA"), or "personally identifying information" as defined or used in New York Education Law 3012-c.

Confidential Information does not include any information that is: (i) lawfully in the public domain at the time of receipt or which lawfully comes into the public domain thereafter through no act of the Vendor,(ii) demonstrated to have been known to the Vendor prior to disclosure by or through the LEA, (iii) disclosed with the prior written approval of the LEA,(iv) demonstrated to have been independently developed by the Vendor without reference to the Confidential Information, (v) disclosed to the Vendor by a third party under conditions permitting such disclosure, and/or (vi) disclosed as required by court order, subpoena, other validly issued administrative or judicial notice or order and/or as a matter of applicable law; provided, however, that in the event disclosure is required of the Vendor under the provision of any law or court order, the Vendor will (a) promptly notify the LEA of the obligations to make such disclosure sufficiently in advance of the disclosure, if possible, to allow the LEA to seek a protective order, and (b) disclose such Confidential Information only to the extent allowed under a protective order, if any, or necessary to comply with the law or court order; Notwithstanding the previous sentence, "personally identifiable information" as defined or used in FERPA or New York Education Law Section 2d,or "personally identifying information" as defined or used in New York Education Law §3012-c remains Confidential Information notwithstanding (A) the applicability of items (i), (ii), (iii) and (vi) in the previous sentence, and (B) items (iv) and (v) of the previous sentence to the extent that such disclosures were made at the direction of or such information was maintained on behalf of the LEA.

FERPA – means the Family and Educational Rights and Privacy Act (20 U.S.C. 1232g) and any applicable regulations promulgated thereunder, including but not limited to 34 C.F.R. Part 99.

Handle -means (in the context of Confidential Information) to create, view, modify, store, transmit or delete.

Local Education Agency (LEA) – means a school district or an educational service agency (e.g. BOCES, RIC).

PII – means personally identifiable information, as defined under FERPA.

System - means any information technology processing device, including routers, servers, Applications, workstations and mobile devices.

Vendor – means **FINANCE MANAGER**, also known as **FINANCE MANAGER** or **FINANCE MANAGER**.

3.0 Relevant Laws, Regulation, Policies and Standards

3.1 Family Education Rights and Privacy Act (FERPA)

FERPA is the primary federal legislation that governs the privacy of educational records. The Vendor must hold all PII obtained, learned or developed by the Vendor in confidence pursuant to applicable provisions of FERPA. The Vendor understands that the release of PII to persons or agencies not authorized to receive such information is a violation of US federal law. Vendor understands that under FERPA it must limit access to PII to those who need to know the Confidential Information for Vendor to perform its duties under its contract, and to destroy all copies of PII, or to return PII to the LEA, when no longer needed or at the expiration of any contract. Vendor understands that upon request, it must permit the LEA access to PII that it holds, in order for the LEA to meet other obligations under FERPA or pursuant to law.

3.2 New York Education Law § 3012-c(IO)

New York Education Law § 3012-c(IO) governs the confidentiality of certain Confidential Information concerning teacher and principal evaluation data. Vendor understands that to the extent that information protected under New York State Education Law §3012-c(IO) is shared with Vendor. Vendor is responsible for complying with this law. Vendor further understands that New York State Education Law § 2-d imposes additional requirements concerning such Confidential Information.

3.3 New York State Education Law § 2-d

New York State Education Law §2-d is a state law that imposes a number of confidentiality and data security requirements in addition to those found in FERPA and New York Education Law §3012-c(IO), including a number of requirements and obligations that apply directly to Vendor. Vendor understands that it is required to comply with the requirements of New York Education Law 2-d and any regulations promulgated thereunder. Vendor understands that among other requirements, New York Education Law

§2-d requires Vendor to:

- Limit internal access to Confidential Information covered under Education Law §2-d ("Covered Confidential Information") to those with legitimate educational interests;
- Not use Covered Confidential Information for any other purposes than those authorized in any contract it is party to;
- Not disclose Covered Confidential Information without parental consent, except to authorized representatives of the Vendor who are carrying out any contract it is party to;
- Maintain reasonable technical, administrative and physical safeguards to protect Covered Confidential Information;
- Not sell covered Confidential Information, nor use Covered Confidential Information for marketing purposes;
- Provide training on laws governing confidentiality to its officers, employees and assignees with access to Covered Confidential Information;
- Use encryption technology to protect Covered Confidential Information while in motion or in its custody from unauthorized disclosure, using a technology or methodology specified under HIPAA by the US Department of Health and Human Services; and
- Notify the LEA of any security breach resulting in an unauthorized release of Covered Confidential Information, and to promptly reimburse LEA for the full notification cost.

Vendor also agrees to cooperate with the LEA in complying with any regulations implementing New York Education Law § 2-d and any LEA or state policies promulgated pursuant to New York Education Law § 2- d, including but not limited to any requirements concerning (a) the inclusion of a data security and privacy plan in Vendor's contract with the LEA,(b) its compliance with any future LEA data privacy/security policy, (c) its compliance with and signature of the Parent Bill of Rights required of the LEA, and (d) the inclusion of supplemental information concerning Vendor's contract in the Parent Bill of Rights.

4.1 0 Privacy, Confidentiality and Internal Controls

FINANCE MANAGER will:

A. **Finance Manager Obligations.** When processing Student Data ("Protected Data") on behalf of Customer, Finance Manager will comply with its obligations under Section 2-d. Finance Manager will.

I. Use Protected Data solely to provide the services under the Agreement and as otherwise described therein;

II. Not disclose Protected Data to any third party (excluding authorized subcontractors) without the prior written consent of the eligible student, parent, teacher, or principal (as applicable);

III. Limit internal access to Protected Data to only those employees or subcontractors that need access to provide the services under the Agreement; and

IV. Not sell Protected Data nor use or disclose it for any marketing or commercial purpose or knowingly permit another party to do so.

B. **Safeguards**. Finance Manager maintains reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its possession, including the following:

I. Finance Manager identifies reasonably foreseeable internal and external risks relevant to its administrative, technical, operational, and physical safeguards.

II. Finance Manager regularly assess the sufficiency of safeguards in place to address identified risks;

III. Finance Manager adjusts its security program in light of business changes or new circumstances;

IV. Finance Manager regularly tests and monitor the effectiveness of key controls, systems, and procedures; and

V. Finance Manager follows written policies to protect against the unauthorized access to or use of Protected Data.

C. Return and/or Destruction of Protected Data. Finance Manager will implement procedures for the return, transition, deletion and/or destruction of Protected Data as follows: Finance Manager deletes all Protected Data within ninety (90) days of expiration of termination of agreement with Customer. For clarity, the Customer, and not Finance Manager, stores and maintains all production copies of Protected Data.

5.1 Incident Response Plan

In the unlikely event an incident occurs where there is a breach or unintended disclosure of Confidential Information or a System that supports it, **FINANCE MANAGER** will adhere to this Incident Response Plan.

D. **Data Security and Privacy Incidents and Obligations**. Finance Manager will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, by following and Incident Response Plan (IRP) for identifying and responding to incidents, breaches, and unauthorized disclosure. Finance Manager will promptly notify Customer of any Breach without unreasonable delay, but no more than seven (7) days after Finance Manager has confirmed or been informed of the breach or unauthorized release.

6.0 Subcontractors

In the event that Finance Manager engages any vendor to process Protected Data, it will (i) conduct due diligence and appropriate risks assessments before first allowing the vendor to access Protected Data, (ii) perform appropriate oversight of such vendor throughout the engagement with the vendor; and (iii) require its vendors to agree to contractual terms to protect Protected Data, including by obligating the vendor to abide by all applicable data protection and security requirements for Protected Data.