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 Vendor 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 Ulster BOCES and Vendor to the contrary, Vendor agrees as follows:

Vendor 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 Vendor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Vendor 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. Vendor 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, Vendor shall have in place sufficient internal controls to ensure that Ulster BOCES' and/or its participants' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, CIPA, FERPA and HIPAA, 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 BOCES and/or a participant. 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 BOCES and/or its Participants as that term is defined in §99.3 of the Family Educational Rights and Privacy Act (FERPA),
>
> -AND-
>
> Personally identifiable information from the records of Ulster BOCES and/or its participants 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.

Vendor 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, Vendor agrees to comply with Ulster BOCES' policy(ies) on data security and privacy. Vendor shall promptly reimburse Ulster BOCES and/or its participants for the full cost of notifying a

parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Vendor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Vendor shall return all of Ulster BOCES' and/or its participants' data, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

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

1. A provision incorporating the requirements of Ulster BOCES' Parents' Bill of Rights for data security and privacy, to the extent that any of the provisions in the Bill of Rights applies to Vendor's possession and use of Protected Data pursuant to this Agreement.

2. An outline of how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the Vendor's policy on data security and privacy.

3. An outline of the measures taken by Vendor to secure Protected Data and to limit access to such data to authorized staff.

4. An outline of how Vendor will use "best practices" and industry standards with respect to data storage, privacy and protection, including, but not limited to encryption, firewalls, passwords, protection of off-site records, and limitations of access to stored data to authorized staff.

5. An outline of how Vendor will ensure that any subcontractors, persons or entities with which Vendor will share Protected Data, if any, will abide by the requirements of Vendor's policy on data security and privacy, and the contractual obligations with respect to Protected Data set forth herein.

DATA PRIVACY AND SECURITY PLAN

1. VENDOR MUST INCLUDE A **SIGNED** COPY OF THEIR DATA & PRIVACY PLAN

2. VENDOR MUST PROVIDE A **SIGNED** COPY OF ULSTER BOCES' BILL OF RIGHTS FOUND ON THE NEXT PAGE.

OnScene Technologies, Inc. Written Information Security Program

1.0 Policy Statement

The OnScene Technologies Written Information Security Program ("WISP") is intended as a set of comprehensive guidelines and policies designed to safeguard all confidential and restricted data maintained at the Company, and to comply with applicable laws and regulations on the protection of Personal Information and Nonpublic Financial Information, as those terms are defined below, found in records and in systems owned by the Company.

2.0 Overview & Purpose

The WISP was implemented to comply with information security standards as requested by our customers.

To satisfy its own and customers' standards, OnScene Technologies will take measures to safeguard personally identifiable information, including financial information, and to provide notice about security breaches of protected information at the company to affected individuals and appropriate state agencies.

OnScene Technologies is committed to protecting the confidentiality of all sensitive data that it maintains, including information about individuals who work at the Company. OnScene Technologies has implemented a number of policies to protect such information, and the WISP should be read in conjunction with these policies that are cross-referenced at the end of this document.

The purposes of this document are to:

- Establish a comprehensive information security program for OnScene Technologies with policies designed to safeguard sensitive data that is maintained by the Company, in compliance with federal and state laws and regulations;
- Establish employee responsibilities in safeguarding data according to its classification level; and
- Establish administrative, technical and physical safeguards to ensure the security of sensitive data.

3.0 Scope

This Program applies to all OnScene Technologies employees, whether full- or part-time, including administrative staff, contract and temporary workers, hired consultants, interns, and customer employees, as well as to all other members of the OnScene Technologies community (hereafter referred to as the "Community"). This program also applies to certain contracted third-party vendors (see section 4.6 for further information). The data covered by this Program includes any information stored, accessed or collected at the Company or for Company operations. The WISP is not intended to supersede any existing OnScene Technologies policy that contains more specific requirements for safeguarding certain types of data, except in the case of Personal Information and Nonpublic

Financial Information, as defined below. If such policy exists and is in conflict with the requirements of the WISP, the other policy takes precedence.

3.1 Definitions

Data

For the purposes of this document, data refers to information stored, accessed or collected at the Company about members of the Community.

Data Custodian

A data custodian is responsible for maintaining the technology infrastructure that supports access to the data, safe custody, transport and storage of the data and provide technical support for its use. A data custodian is also responsible for implementation of the business rules established by the data steward.

Data Steward

A data steward is responsible for the data content and development of associated business rules, including authorizing access to the data.

Personal Information

Personal Information ("PI"), as defined by Massachusetts law (201 CMR 17.00), is the first name and last name or first initial and last name of a person in combination with any one or more of the following:

- Social Security number;
- Driver's license number or state-issued identification card number; or
- Financial account number (e.g. bank account) or credit or debit card number that would permit access to a person's financial account, with or without any required security code, access code, personal identification number, or password.

For the purposes of this Program, PI also includes passport number, alien registration number or other government-issued identification number.

Nonpublic Financial Information

The GLB Act (FTC 16 CFR Part 313) requires the protection of "customer information", that applies to any record containing nonpublic financial information ("NFI") about a customer or other third party who has a relationship with the Company, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the Company. For these purposes, NFI shall include any information:

- A customer or other third party provides in order to obtain a financial product or service from the Company;
- About a customer or other third party resulting from any transaction with the Company involving a financial product or service; or
- Otherwise obtained about a customer or other third party in connection with providing a financial product or service to that person.

Examples of NFI include:

- Information a consumer provides to you on an application to obtain a loan, credit card, or other financial product or service;
- Account balance information, payment history, overdraft history, and credit or debit card purchase information;
- The fact that an individual is or has been one of your customers or has obtained a financial product or service from you;
- Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;
- Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;
- Any information you collect through an Internet "cookie" (an information collecting device from a web server); and
- Information from a consumer report.

3.2 Data Classification

All data covered by this policy will be classified into one of three categories outlined below, based on the level of security required for each, starting with the highest level.

Confidential

Confidential data refers to any data where unauthorized access, use, alteration or disclosure of this data could present a significant level of risk to OnScene Technologies or the Community. Confidential data should be treated with the highest level of security to ensure the privacy of that data and prevent any unauthorized access, use, alteration or disclosure.

Confidential data includes data that is protected by the following federal or state laws or regulations: 201CMR17.00 (Mass Security Regs), 16 CFR 313 (Privacy of Consumer Financial Information), the Federal Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the FTC's Red Flag Rules. Information protected by these laws includes, but is not limited to, PI, NFI and Protected Health Information (PHI).

Restricted

Restricted data refers to all other personal and institutional data where the loss of such data could harm an individual's right to privacy or negatively impact the finances, operations or reputation of OnScene Technologies. Any non-public data that is not explicitly designated as Confidential should be treated as Restricted data.

Restricted data includes data protected by the Family Educational Rights and Privacy Act (FERPA), referred to as student education records. This data also includes, but is not limited to, intellectual property (proprietary research, patents,

etc.), Company financial and investment records, employee salary information, or information related to legal or disciplinary matters.

Restricted data should be limited to access by individuals who are employed by OnScene Technologies and who have legitimate reasons for accessing such data, as governed by FERPA, or other applicable law or Company policy. A reasonable level of security should be applied to this classification to ensure the privacy and integrity of this data.

Public (or Unrestricted)

Public data includes any information for which there is no restriction to its distribution, and where the loss or public use of such data would not present any harm to OnScene Technologies or members of the OnScene Technologies community. Any data that is not classified as Confidential or Restricted should be considered Public data.

4.0 Policy

4.1 Responsibilities

All data at the Company is assigned a data steward according to the constituency it represents. Data stewards are responsible for approval of all requests for access to such data. Currently the Company's Chief Information Officer (CIO) is the data steward for all data and Information Technology Services (ITS) staff serve as the data custodians for all data.

Human Resources will inform ITS staff about an employee's change of status or termination as soon as is practicable but before an employee's departure date from the Company. Changes in status may include terminations, leaves of absence, significant changes in position responsibilities, transfer to another department, or any other change that might affect an employee's access to Company data. For detailed information regarding account terminations, see the Electronic Content Stewardship Policy.

The ITS Security Team is in charge of maintaining, updating, and implementing this Program. The Company's CIO has overall responsibility for this Program.

All members of the Community are responsible for maintaining the privacy and integrity of all sensitive data as defined above, and must protect the data from unauthorized use, access, disclosure or alteration. All members of the Community are required to access, store and maintain records containing sensitive data in compliance with this Program.

4.2 Identification and Assessment of Risks to Company Information

OnScene Technologies recognizes that it has both internal and external risks to the privacy and integrity of Company information. These risks include, but are not limited to:

- Unauthorized access of Confidential data by someone other than the owner of such data

- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of Confidential data by employees
- Unauthorized requests for Confidential data
- Unauthorized access through hard copy files or reports
- Unauthorized transfer of Confidential data through third parties

OnScene Technologies recognizes that this may not be a complete list of the risks associated with the protection of Confidential data. Since technology growth is not static, new risks are created regularly. Accordingly, ITS will actively participate and monitor advisory groups such as the Educause Security Institute, the Internet2 Security Working Group and SANS for identification of new risks.

OnScene Technologies believes the Company's current safeguards are reasonable and, in light of current risk assessments made by ITS, are sufficient to provide security and confidentiality to Confidential data maintained by the Company. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

4.3 Policies for Safeguarding Confidential Data

To protect Company data classified as Confidential, the following policies and procedures have been developed that relate to access, storage, transportation and destruction of records. For an overview of storage guidelines, see the Data Storage Guide.

Access & Storage

- Only those employees or authorized third parties requiring access to Confidential data in the regular course of their duties are granted access to this data, including both physical and electronic records.
- To the extent possible, all electronic records containing Confidential data should only be stored in the Company's cloud storage services and not on local machines or unsecured servers.
- PHI may be stored or accessed through the Google Apps core suite (including Mail, Drive, Groups, Sites, Chat) as these apps are certified HIPAA compliant, provided that access to the PHI is appropriately restricted. This does not apply to Google consumer apps such as Google+, Hangouts, etc.
- Massachusetts PI and NFI must not be stored on any Google app.
- Confidential data must not be stored on cloud-based storage solutions that are unsupported by the Company (including DropBox, Microsoft OneDrive, Apple iCloud, etc.).

- Members of the Community are strongly discouraged from storing Confidential data on laptops or on other mobile devices (e.g., flash drives, smart phones, external hard drives). However, if it is necessary to transport Confidential data electronically, the mobile device containing the data must be encrypted.
- Paper records containing Confidential data must be kept in locked files or other secured areas when not in use.
- Upon termination of employment or relationship with OnScene Technologies, electronic and physical access to documents, systems or other network resources containing Confidential data is immediately terminated. (See the Stewardship of Electronic Content Policy for more information.)

Transporting Confidential Data

- Members of the Community are strongly discouraged from removing records containing Confidential data off premises. In rare cases where it is necessary to do so, the user must take all reasonable precautions to safeguard the data. Under no circumstances are documents, electronic devices, or digital media containing Confidential data to be left unattended in any unsecure location.
- When there is a legitimate need to provide records containing Confidential data to a third party outside OnScene Technologies, electronic records shall be password-protected and/or encrypted, and paper records shall be marked confidential and securely sealed.

Destruction of Confidential Data

- Records containing Confidential data must be destroyed once they are no longer needed for business purposes, unless state or federal regulations require maintaining these records for a prescribed period of time.
- Paper and electronic records containing Confidential data must be destroyed in a manner that prevents recovery of the data. Massachusetts General Law 93I specifies the manner in which records containing PI must be destroyed.

4.4 Policies for Safeguarding Restricted Data

- Access to Restricted Data should be limited to members of the Community who have a legitimate business need for the data.
- Restricted Data can be stored on AWS, Microsoft Azure, or Google Cloud Platform.
- Restricted Data may be stored on cloud-based storage solutions that are unsupported by the Company as long as they are in compliance with the requirements of any laws governing the protection of such data (e.g., FERPA).
- Documents containing Restricted Data should not be posted publicly.

4.5 Password Requirements

In order to protect Company data, all members of the Community must select unique passwords following the standards set by NIST Special Publication

800-63-3 - Digital Identity Guidelines:

- Has at least 8 characters, up to 64 characters
- Does not contain any part of the user's name, username (e.g., Jill1230)
- Does not appear in known password dictionaries
- Encourages use of long, easy to remember phrases
- Members of the community must protect the privacy of their passwords. Passwords must not be shared with others. If an account or password is suspected to have been compromised, all passwords should be changed immediately and the incident reported to the OnScene Technologies Help Desk.

4.6 Third-Party Vendor Agreements Concerning Protection of Personal Information

OnScene Technologies exercises appropriate diligence in selecting service providers capable of maintaining appropriate security safeguards for PI provided by the Company to them. The primary budget holder for each department is responsible for identifying those third parties providing services to the Company that have access to PI. All relevant contracts with these third parties are reviewed and approved by the OnScene Technologies Purchasing Department to ensure the contracts contain the necessary language regarding safeguarding PI. It is the responsibility of the primary budget holders to confirm that the third parties are required to maintain appropriate security measures to protect PI consistent with this Program and Massachusetts laws and regulations.

4.7 Computer system safeguards

Technology Support Services staff monitor and assess safeguards on an ongoing basis to determine when enhancements are required. The Company has implemented the following to combat external risk and secure the Company network and systems containing Confidential Data:

- Secure user authentication protocols:
  - Unique passwords are required for all user accounts; each employee receives an individual user account.
  - Server accounts are locked after multiple unsuccessful password attempts.
  - Computer access passwords are disabled upon an employee's termination.
  - User passwords are stored in an encrypted format; root passwords are only accessible by system administrators.
- Secure access control measures:
  - Access to specific files or databases containing Confidential Data is limited to those employees who require such access in the normal course of their duties.
- Operating system patches and security updates are installed to all servers on a regular basis.
- User access and activity is logged and kept for at least 30 days.

- Antivirus and anti-malware software is installed and kept updated on all workstations.

4.8 Employee Training

All administrative employees are required to complete the online or in-person security training "Securing the Human" on an annual basis. Any customer or contract employee that has access to PI is also required to complete this yearly training. The training is also strongly recommended for all employees.

Additionally, users who are the victims of a phishing attack will be required to complete this course within 2 weeks after ITS identifies the issue, regardless of whether or not they have already completed the training. If a user fails to complete the training within 2 weeks, his or her remote access to Company resources will be disabled. The ITS Security Team maintains records of all such training.

4.9 Reporting Attempted or Actual Breaches of Security

Any incident of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of PI, or of a breach or attempted breach of the information safeguards adopted under this Program, must be reported immediately to the CIO. The CIO will contact the Risk and Compliance Manager (RCM), who will convene the Data Incident Team. The RCM is responsible for coordinating the Data Incident Team and determining appropriate actions in their response to the breach. The Incident Team will document all breaches and subsequent responsive actions taken. All related documentation will be stored in the Finance Office.

For more information about incident response, including specific procedures for responding to a breach, see the OnScene Technologies Data Incident Response Plan.

5.0 Enforcement

Any employee or customer who willfully accesses, discloses, misuses, alters, destroys, or otherwise compromises Confidential or Restricted data without authorization, or who fails to comply with this Program in any other respect, will be subject to disciplinary action, which may include termination in the case of employees and expulsion in the case of customers.

6.0 Policies cross-referenced

The following OnScene Technologies policies provide advice and guidance that relates to this Program:

- Acceptable Use Policy
- Data Incident Response Plan
- Employee Confidentiality Policy
- FERPA Policy
- HIPAA Privacy Policy

- Identity Theft Prevention Policy ("Red Flag Rules")

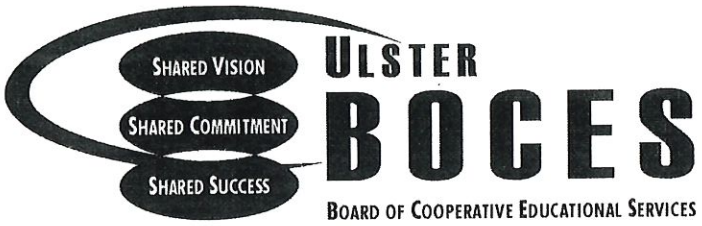
7.0 Effective date

This Written Information Security Program was implemented December 1, 2019. Revisions: none.

The Company will review this Program at least annually and reserves the right to change, modify, or otherwise alter this Program at its sole discretion and at any time as it deems circumstances warrant.

ERIK ENDRESS

CEO



Parents Bill of Rights - Data Privacy & Security

The Agency is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with Education Law § 2-d, the Agency wishes to inform the school community of the following:

1. A student's personally identifiable information cannot be sold or released for any 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 will be available for public review at a later date.

5. Parents have the right to have complaints about possible breaches of student data addressed. More information about where to address those complaints will be provided at a later date.

Signature: DocuSigned by Erik Endress

Print Name: Erik Endress

Title: CEO

Company Name: OnScene Technologies, Inc

Date: 3/16/2021

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: DocuSigned by Erik Endress

Print Name: Erik Endress

Title: CEO

Company Name: OnScene Technologies, Inc

Date: 3/16/2021