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 Day Automation Systems (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 may 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: Day Automation Systems

BY: Danie Macaro **DATED:** 4/18/2023

DATA PRIVACY AND SECURITY PLAN

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

Day Automation Systems, Inc.

Data Security and Privacy Plan

Version 1.0 - 21MAR2023

Table of Contents

Table of Contents.....2

1.0 Purpose.....3

2.0 Terminology.....3

3.0 Relevant Laws, Regulation, Policies and Standards.....4

3.1 Family Education Rights and Privacy Act {FERPA).....4

3.2 New York Education Law § 3012-c(10).....4

3.3 New York State Education Law § 2-d.....4

4.0 Privacy, Confidentiality, and Internal Controls.....5

5.0 Incident Response Plan.....6

6.0 Subcontractors.....6

1.0 Purpose

The purpose of this Data Security and Privacy Plan is to document **Day Automation's** 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 **Day Automation's** provided 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 including, but is not limited to, their names, addresses, contact information, school or school attended, school district, grades or other reviews, credits, scores, analysis or evaluations, student or employee records, relevant 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; 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.

Day Automation may not disclose Confidential Information except to the extent such Confidential Information 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, **Day Automation** shall not disclose any "personally identifiable information" as defined or used in FERPA or New York Education Law Section 2-d and its implementing regulations (8 NYCRR Part 121),or "personally identifying information" as defined or used in New York Education Law §3012-c to any other party without the prior written consent of the parent or eligible student 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 LEA; or unless required by statute or court order and **Day Automation** has provided a notice of disclosure to the department, LEA 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 statute or court order.

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 **Day Automation**, also known as **Day Automation Systems, Inc.,** also known as **Day**.

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(10)

New York Education Law § 3012-c(10) 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(10) 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 the confidentiality of teacher and principal evaluation data.

3.3 New York State Education Law § 2-d

New York State Education Law §2-d imposes a number of confidentiality and data security requirements in addition to those found in FERPA and New York Education Law §3012-c(10), 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 its implementing regulations (8 NYCRR Part 121), which require Vendor to:

- Limit internal access to Confidential Information covered under Education Law §2-d ("Covered Confidential Information") to those employees or sub-contractors that need access to provide the contracted services.
- Not use Covered Confidential Information for any other purposes than those explicitly authorized in the contract.
- Not disclose Covered Confidential Information to any other party without the prior written consent of the parent or eligible student, except to authorized representatives of the Vendor to the extent they are carrying out the contract and in compliance with state and federal law, regulations, and the contract, or unless required by statute or court order and the Vendor provides a notice of disclosure to Ulster County BOCES no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order;
- Maintain reasonable technical, administrative and physical safeguards to protect the security, confidentiality and integrity of Covered Confidential Information;
- Not sell covered Confidential Information, nor use Covered Confidential Information 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;
- 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;
- 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;
- Adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

Vendor also agrees to cooperate with the LEA in complying with the regulations implementing New York Education Law § 2-d (i.e. 8 NYCRR Part 121) 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 the LEA's Data Security and Privacy 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. Vendor acknowledges that it has been provided access to the LEA's Data Security and Privacy Policy and has reviewed same.

4.0 Privacy, Confidentiality, and Internal Controls

Day Automation will:

A. Comply with LEA's Data Security and Privacy Policy, in addition to all laws, regulations, policies and standards listed in Section 3.0 of this Data Security and Privacy Plan by: Ensuring that all protected data is stored on the local district infrastructure. The LEA owns, maintains, and is responsible for granting access to authorized individuals. The LEA data privacy policy in place shall prevail over any Day Automation policy. PII may be stored within our AWS cloud-based services for the sole use of providing backup and restoration services only unless prior customer written instruction is received directing otherwise. All other access will be for the sole purpose of authorized use of our maintenance services without the collection of PII.

B. Hold Confidential Information in strict confidence, limit internal access to it to those employees or sub-contractors that need access to provide the contracted services (via administrative processes and Application and System authentication mechanisms), and not disclose it to any third parties nor make use of such Data for its own benefit or for the benefit of another, or for any use other than the purpose agreed upon with the LEA.

C. Provide training on federal and state law governing Confidential Information to any officers, employees, or assignees prior to them having access to Confidential Information.

    i. Training is assigned to applicable staff upon authorization to access PII.

        - Annual refresher training is provided subsequently.

D. Use commercially reasonable efforts to secure and defend any System housing Confidential Information against third parties who may seek to breach the security thereof, including, but not limited to breaches by unauthorized access or making unauthorized modifications to such System, that will involve at least the following best practice technology approaches:

    i. Dual Factor Authentication

    ii. Virtual Private Network (VPN) Connections

    iii. Recurring cybersecurity awareness training

    iv. Restricted access to secured data

    v. 24/7 systems monitoring via extended detection and response (XDR)

E. Protect and secure all Confidential Information in transit (collected, copied and moved) and at rest (stored on the physical servers), including during any electronic data transmission or electronic or physical media transfer.

F. Maintain all copies or reproductions of Confidential Information with the same security it maintains the originals, and at the point in which the Confidential Information is no longer useful for its primary or retention purposes, as specified by the LEA, will destroy such Data, making it unusable and unrecoverable; and

G. Ensure Confidential Information will not appear in URLs of any Application.

H. Day Automation shall destroy/delete the data when the contract is terminated or expires, or upon written instruction by the LEA.

5.0 Incident Response Plan

In the event an incident occurs where there is a breach or unintended disclosure of Confidential Information or a System that contains Confidential Information, **Day Automation** will adhere to this Incident Response Plan:

A. **Day Automation** will comply with all applicable breach notification laws, including New York State Education Law § 2-d, Part 121 of the Commissioner's Regulations, and the New York State Data Breach Notification Act (General Business Law §899-aa and New York State Technology Law § 208, as appropriate).

B. **Day Automation** will promptly notify the LEA in the most expedient way possible and without unreasonable delay but no more than 24 hours of the discovery of a breach or unintended disclosure of Confidential Information or a System that supports it. Such notification shall be by email and either certified mail, return receipt requested, or overnight mail.

C. **Day Automation** will cooperate with the LEA and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Confidential Information.

D. Response actions to incidents that might affect Confidential Information or Systems will be conducted quickly and with ample resources. **Day Automation** may hire a professional third-party incident response team if in-house resources do not have sufficient skill or availability.

D. **Day Automation** will provide the LEA with the opportunity to view available incident response evidence, reports, communications, and related materials associated with the respective incident, if they so request.

E. If requested by the LEA, or if required by law, **Day Automation** will notify in writing all persons affected by the incident, at its own cost and expense and/or pay for or promptly reimburse the LEA for the full costs of any notifications required by law as a result of a breach or unauthorized release attributed to Day Automation.

6.0 Subcontractors

Day Automation will not utilize subcontractors. In the event that **Day Automation** utilizes subcontractors to support a System that Handles Confidential Information (each a "subcontractor") to provide the contracted services, **Day Automation** shall ensure that any such subcontractor will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., FERPA, Education Law §2-d) that are imposed on **Day Automation** by the completion and submission of an executed contractual rider document as an amendment to the Day Automation contractual agreement on file with the LEA.

Supplemental Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, Ulster County BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract the LEA enters into with a third-party contractor where the third party contractor receives student data or teacher or principal data will include supplemental information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used, as defined in the contract.
2. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements;
3. The duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or principal data upon expiration of the agreement (e.g., whether, when and in what format it will be returned to Ulster County BOCES, and/or whether, when and how the data will be destroyed);
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; and
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. How the data will be protected using encryption while in motion and at rest.

The Supplemental Information elements listed above have been developed for the contract between Ulster County BOCES and the Company and are hereby incorporated by reference into this Data Security and Privacy Plan.

The Company shall:

1. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
2. Limit internal access to education records to those individuals who have a legitimate

educational interest in such records.

3. Not use educational records for any other purpose than those explicitly authorized in the contract;
4. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
5. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody.
6. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
7. Notify Ulster County BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay.
8. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract.
9. Provide a signed copy of this Bill of Rights to Ulster County BOCES thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

Company hereby acknowledges that it is aware of and agrees to abide by the terms of the Ulster County BOCES' Parents Bill of Rights for Data Privacy and Security.

SIGNATURE: Daniel Vaccaro

PRINTED NAME: Daniel Vaccaro

TITLE: Chief Compliance Officer

COMPANY NAME: Day Automation Systems, Inc.

DATE: 4/18/2023

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 §2-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 Regarding Third Party 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, third-party 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: Daniel Vaccaro

Print Name: Daniel Vaccaro

Title: Chief Compliance Officer

Company Name: Day Automation Systems

Date: 4/17/2023