EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING

BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

AND

SUPPLEMENTAL INFORMATION ABOUT A CONTRACT

BETWEEN PROFESSIONAL SOFTWARE FOR NURSES, INC. AND ERIE 1 BOCES

1. **Purpose**

(a) This Exhibit D sets forth the terms of a Data Sharing and Confidentiality Agreement ("DSC Agreement") that has been agreed to by the Parties as a supplement to the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and Part 121 of the Regulations of the NYS Commissioner of Education (collectively referred to as "Section 2-d"). This DSC Agreement consists of the data sharing and confidentiality terms set forth herein, a copy of "Erie 1 BOCES' Bill of Rights for Data Security and Privacy" signed by the Vendor, and the "Supplemental Information about a Contract between Vendor and Erie 1 BOCES" that is required to be posted on Erie 1 BOCES' website.

(b) Vendor shall comply with all terms, conditions and obligations as set forth in this DSC Agreement, including within the Erie 1 BOCES' Bill of Rights for Data Security and Privacy and the Supplemental Information about a Contract between Vendor and Erie 1 BOCES, throughout the duration of the term of the MLSA to which it is attached. The terms of this DSC Agreement shall supersede and take the place of any other data sharing and confidentiality agreement or any similar data sharing and confidentiality language previously agreed to by the Parties prior to the date of mutual execution of the MLSA to which this DSC Agreement is attached as an Exhibit.

(c) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this DSC Agreement, the terms of this DSC Agreement will apply and be given effect. In the event that Vendor has online or written Privacy Policies or Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this DSC Agreement, the terms of this DSC Agreement will apply and be given effect.

2. **Definitions**

Any capitalized term used within this DSC Agreement that is also found in the MLSA, if any will have the same definition as contained within the MLSA.

In addition, as used in this DSC Agreement:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

(d) "Participating Educational Agency" means a school, school district or BOCES within New York State that purchases certain shared technology services and software through a Cooperative Educational Services Agreement ("CoSer") with Erie 1 BOCES, and as a result is licensed or granted access to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this DSC Agreement, the term also includes Erie 1 BOCES if licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

(e) "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located within New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of all Protected Data it receives in accordance with applicable federal and state law (including but not limited to Section 2-d) and this DSC Agreement, as may be amended by the Parties, and Erie 1 BOCES' policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy, and that Erie 1 BOCES will provide Vendor with a copy of its policy upon request.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy, and security of the Protected Data it receives from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this DSC Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this DSC Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

(b) As required by the NIST Cybersecurity Framework, in order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational, and physical safeguards and practices in place throughout the term of the MLSA:

Data Security:

- Data-at-rest & data-in-transit is encrypted
- Data leak protections are implemented

Information Protection Processes and Procedures:

- Data destruction is performed according to contract and agreements
- A plan for vulnerability management is developed and implemented

Protective Technology:

- Log/audit records are ascertained, implemented, documented, and reviewed according to policy
- Network communications are protected

Identity Management, Authentication and Access Control:

- Credentials and identities are issued, verified, managed, audited, and revoked, as applicable, for authorized devices, processes, and users
- Remote access is managed

(c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about a Contract between Vendor and Erie 1 BOCES," below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(e) Vendor _____will ___X_will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about a Contract between Vendor and Erie 1 BOCES," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this DSC Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in the "Supplemental Information about a Contract between Vendor and Erie 1 BOCES," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this DSC Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.

(c) Not use Protected Data for any purposes other than those explicitly authorized in this DSC Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:

(i) the parent or eligible student has provided prior written consent; or
(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to the Participating Educational Agency no later than the time of disclosure unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in the "Supplemental Information about a Contract between Vendor and Erie 1 BOCES," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this DSC Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse Erie 1 BOCES or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students,

teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

(a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to Erie 1 BOCES by contacting the designated BOCES contact at the email address, telephone number, and/or mailing address provided by Customer.

(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to the designated BOCES Contact about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist Erie 1 BOCES or its Participating Districts that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform the designated BOCES contact.

(e) Vendor will consult directly with the designated BOCES contact prior to providing any further notice of the incident (written or otherwise) directly to any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)

ERIE 1 BOCES

BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the 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 is available for public review at http://www.nysed.gov/data-privacy-security/student-data-inventory, 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 the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website: http://www.nysed.gov/data-privacy-security/report-improper-disclosure.

BY THE VENDOR:

Peter Redes

Signature

CEO

Title

March 14, 2023

Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION ABOUT A CONTRACT

BETWEEN PROFESSIONAL SOFTWARE FOR NURSES, INC. AND ERIE 1 BOCES

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with Professional Software for Nurses, Inc. which governs the availability to Participating Educational Agencies of the following Product(s):

SNAP Health Center

Pursuant to this MLSA, Participating Educational Agencies (*i.e.*, those educational agencies that are authorized to use the above Product(s) by purchasing certain shared technology services and software through a Cooperative Educational Services Agreement with Erie 1 BOCES) may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data"). The MLSA incorporates a Data Sharing and Confidentiality Agreement ("DSC Agreement") with Erie 1 BOCES setting forth Vendor's obligations to protect the confidentiality, privacy, and security of Protected Data it receives pursuant to the MLSA.

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA, including the DSC Agreement. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging their obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: Subcontractors will not be used.

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on July 1, 2023, and expires on June 30, 2026.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.
- In the event the MLSA is assigned to a successor Vendor (to the extent authorized by the MLSA), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

Attachment A

Professional Software for Nurses, Inc.

Disaster Recovery Plan

Section of: Corporate Policies

Created By: D. Savina | Modified By: M. Pescuma

Last Revision Date: January 20, 2022

Last Approved By: P. Redes on February 8, 2023

Confidentiality Notice

Table of Contents

Professional Software for Nurses is hereinafter referred to as "the company."

1.0 Overview

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives PSNI a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. The Disaster Recovery Plan is often part of the Business Continuity Plan.

2.0 Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by PSNI that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

3.0 Scope

This policy is directed to the Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

4.0 Policy

4.1 Contingency Plans

This plan should cover:

- Short term events:
  - Power loss
  - Server room cooling failure
  - Internet provider disruption
  - Equipment failure
  - Building damage
- Long term events:
  - Extended power loss
  - Internet provider loss
  - Building loss

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Table top exercises should be conducted to determine issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, should be reviewed an updated on an annual basis.

4.2 Computer Emergency Response Plan

Response to emergency events:

- Power loss:
  - Alarm monitoring service will notify responsible employee.
  - CEO and VP technology will receive text message alert via Cell phone that backup generator is operational.
  - If backup generator is running normally then no action is needed. For long term outage propane delivery may be required. If backup generator fails:
    - Responsible party will contact backup generator service provider for service.
    - Tech support will continue to handle customer calls from remote location.
    - Customers will be notified regarding service interruption.
- Primary cooling fails causing over temperature in server room:
  - A redundant cooling system is installed that will provide adequate cooling.
  - Should the backup cooling system fail:
    - Alarm monitoring service will notify responsible employee.
    - Responsible employee will arrange for ventilation of server room and contact VP technology if over temperature condition continues.
  - Contact HVAC for service.
- Building fire:
  - Alarm monitoring service will notify responsible employee.
  - Local fire department will respond as well as responsible employee.
  - Server room fire:
    - Fire suppression system will automatically activate.
    - Secondary audible alarm will sound.
  - Severity of fire:
    - Minimal – Business continues as close to normal as possible.
    - Extensive damage (server room intact) – Employees work remotely until damage is repaired.
    - Loss of server room
      - Using backup data, recreate necessary infrastructure in cloud provider data center.
      - Evaluate damage and purchase replacement equipment.
      - Tech support will continue to handle customer calls from remote location.
      - Customers will be notified regarding service interruption.
    - Total loss
      - Using backup data, recreate necessary infrastructure in cloud provider data center.
      - Employees work remotely until damage is repaired.
      - Customers will be notified regarding service interruption.
  - Any necessary repairs and/or replacements will be coordinated by the CEO.
- Intrusion during off hours:
  - Alarm monitoring service will notify responsible employee.
  - Responsible employee will proceed to office and enable police to check cause of alarm.
  - Determine any damage and/or loss and take necessary action for recovery/replacement.
- Primary internet connectivity loss:
  - CEO and VP technology will receive email message and determine approach to resolve.
  - Contact internet service provider.
  - Secondary internet connection will handle all traffic.
  - Secondary internet connection fails:
    - Customers will be notified regarding service interruption.
    - Short-term outage
      - Tech support will continue to handle customer calls from remote location.
    - Long-term outage
      - Using backup data, recreate necessary infrastructure in cloud provider data center.
      - Employees work remotely until connectivity is restored.
- Equipment failure:
  - All equipment is configured with redundancy.

    - Redundant equipment fails:
        - Evaluate failure and purchase replacement equipment.
        - Customers will be notified regarding service interruption.
- Natural disaster/unforeseen/other – Action will be determined based on event.

4.3 Succession Plan

Flow of responsibility when normal staff is unavailable to perform their duties will follow up the organization chart.

4.4 Data Study

All client databases that are stored on the cloud servers are to be considered confidential. Company financial and human relations files store on the business server are to be considered confidential. Nightly backup to a cloud (FirstLight and Azure(client Databases only)) location in addition to the local backups are to be performed.

4.5 Applicability of Other Policies

This document is part of the PSNI's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

4.6 Criticality of Service List

Services provided and their order of importance.

- Client databases and applications.
- Customer tracking and authentication applications.
- Company financial applications and databases.

Equipment Replacement Plan: the following equipment is needed as a minimum to provide client service. This list will be updated annually.

1x FortiGate 100F Firewall
2x Ruckus ICX 7250-48p Switch
1x Barracuda 340 Load Balancer
1x Dell EMC SCV3020 SAN
1x Disk Tray SVc320
1x Synology RackStation RS2818RP+
7x Servers (Dual Processor)

4.7 Business Continuity Testing

Business Continuity Testing should be performed annually via a tabletop exercise.

5.0 Enforcement

The management team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback to the policy owner.

5.1 Exceptions

Any exception to the policy must be approved by the management team in advance.

6.0 Definitions

Emergency event Any reasonable event that can interrupt service of cloud service to PSNI Clients.

7.0 Revision History

Date	Rev	Description of change	Originator	Approvers
May 2016	1	Policy Creation	D. Savina	P. Redes
Jan 2017	1	Review		P. Redes
Jan 2018	1	Review		P. Redes
Jan 2019	1	Review		P. Redes
June 2019	1.1	Review		P. Redes
May 2020	1.2	Review and update		P. Redes
October 2020	1.3	Revised ERP	D. Savina	P. Redes
January 2022	1.4	Removed mention of tapes and added some required minimum equipment.	M. Pescuma	P. Redes
December 2022	1.4	Review	M. Pescuma	P. Redes