STANDARD STUDENT DATA PRIVACY AGREEMENT

NEW YORK

NY-NDPA, Standard Version 1.0

Webster Central School District

and

Delphi Drug & Alcohol Council Inc

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between: Webster Central School District, located at 119 South Ave, Webster, NY 14580 USA (the "**Local Education Agency**" or "**LEA**") and Delphi Drug & Alcohol Council Inc, located at 72 Hinchey Rd, Rochester, NY 14624 USA (the "**Provider**").

WHEREAS, the Provider is providing educational or digital services to LEA.
WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and
WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.
NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions.** ***Check if Required***

   √ If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.

   √ If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.

4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.

5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**").

6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: Jennifer Cathy Title: President and CEO

Address: 72 Hinchey Road Rochester, NY 14624

Phone: 585-355-7842 Email: jcathy@delphirise.org

The designated representative for the LEA for this DPA is:

Brian Zimmer, Data Privacy Officer

Phone: 585-216-0099

Address: 119 South Ave, Webster, NY 14580

Email: brian_zimmer@webstercsd.org

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

Webster Central School District

By: _____ Date: 09/02/2025

Printed Name: Brian Zimmer Title/Position: Director of Educational Technology/DPC

Delphi Drug & Alcohol Council Inc

By: _____ Date: 9/2/2025

Printed Name: Jennifer Cathy Title/Position: President and CEO

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data

2. **Student Data to Be Provided**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.

3. **DPA Definitions**. The definition of terms used in this DPA is found in **Exhibit "C".** In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.

2. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the

Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.

3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.

2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.

3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D.

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security**. The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

4. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

(1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

i. The name and contact information of the reporting LEA subject to this section.
ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

(3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

(5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination**. In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.

2. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.

3. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement**. This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

6. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

7. **Successors Bound**: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of

all or substantially all of the assets of such business In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

9. **Waiver**. No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT “A”
DESCRIPTION OF SERVICES

Schools in the Rochester New York area collaborate with Delphi Rise to provide school-based prevention and counseling services, including individual and group therapy, evidence-based programs, and educational workshops, aimed at reducing substance use and promoting mental wellness among students. These services are offered at no cost and are designed to support students who may not otherwise have access to such resources. Delphi Rise's trauma-informed approach ensures that interventions are sensitive to the effects of adverse childhood experiences.

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	X
	Place of Birth	
	Gender	X
	Ethnicity or race	X
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	X
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	X
	Email	
	Phone	X
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	X

Category of Data	Elements	Check if Used by Your System
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	X
	Email	X
	Phone	X
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	X
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	

Category of Data	Elements	Check if Used by Your System
	Student bus card ID number	
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application:	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

EXHIBIT "C"
DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline

records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

[**Insert Name of District or LEA**] Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

_____ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[**Insert categories of data here**]

_____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

_____ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[**Insert or attach special instructions**]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By [**Insert Date**]

4. Signature

_____ _____

Authorized Representative of LEA Date

5. Verification of Disposition of Data

_____ _____

Authorized Representative of Company Date

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
☑	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
☐	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
☐	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
☐	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
☐	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
☐	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Exhibit "G"
New York

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New York. Specifically, those laws are New York Education Law § 2-d; and the Regulations of the Commissioner of Education at 8 NYCRR Part 121; and

WHEREAS, the Parties wish to enter into these additional terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New York;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.

2. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the DPA.

3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA's Data Security and Privacy Policy. The LEA's Data Security Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security Policy to the Provider upon execution of Exhibit "E". Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations.

4. Provider represents that their Data Privacy and Security Plan can be found at the URL link listed in Exhibit K and is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a)implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the service agreement; (c) complies with the LEA's parents bill of rights for data privacy and security; (d) requires training of all providers' employees, assignees and subprocessors who have Access to student data or APPR data; (e) ensures subprocessors are required to protect PII received under this service agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, deletion and destruction.

5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit "E".

6. All references in the DPA to "Student Data" shall be amended to include and state, "Student Data and APPR Data."

7. To amend Article II, Section 5 to add: Provider shall ensure that its subprocessors agree that they do not have any property, licensing or ownership rights or claims to Student Data or APPR data and that they will comply with the LEA's Data Privacy and Security Policy. Provider shall examine the data privacy and security measures of its Subprocessors. If at any point a Subprocessor fails to materially comply with the requirements of this DPA, Provider shall: (i) notify LEA, (ii) as applicable, remove such Subprocessor's Access to Student Data and APPR Data; and (iii) as applicable, retrieve all Student Data and APPR Data received or stored by such Subprocessor and/or ensure that Student Data and APPR Data has been securely deleted or securely destroyed in accordance with this DPA. In the event there is an incident in which Student Data and APPR Data held, possessed, or stored by the Subprocessor is compromised, or unlawfully Accessed or disclosed, Provider shall follow the Data Breach reporting requirements set forth in the DPA.

8. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."

9. To amend Article IV, Section 3 to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data and APPR Data will be trained on the federal and state laws governing confidentiality of such Student Data and APPR Data prior to receipt. Access to or Disclosure of Student Data and APPR Data shall only be provided to Provider's employees and subprocessors who need to know the Student Data and APPR Data to provide the services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide such services.

10. To replace Article IV, Section 6 (Disposition of Data) with the following: Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider's certifying that it and it's subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any assurance of discontinuation, which will control in the case of a conflict.

    Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all student data after providing the LEA with ninety (90) days prior notice.

The duty to dispose of student data shall not extend to Student Data that had been de-identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "**Directive for Disposition of Data"** form, a copy of which is attached hereto as **Exhibit "D",** or, with reasonable notice to the Provider, other form of its choosing. No further written request or notice is required on the part of either party prior to the disposition of Student Data described in **"Exhibit D".**

11. To amend Article IV, Section 7 to add: 'Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, "which term shall not include students."

12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States, European Union, and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

13. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an unauthorized Access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA or its designee(s) to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA or its designee(s) and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable Access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.

Upon request by the New York State Education Department's Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require Provider to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider's expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider's privacy and security practices that was issued no more than twelve months before the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the NIST Cybersecurity Framework v1.1 or any update to this Framework that is adopted by the New York State Department of Education.

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

    (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

    i. The name and contact information of the reporting LEA subject to this section.

    ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

    iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

    iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and

    v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

    vi. The number of records affected, if known; and

    vii. A description of the investigation undertaken so far; and

    viii. The name of a point of contact for Provider.

    (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

    (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

    (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals.

    (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

    (6) Provider and its subprocessors will cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

15. To amend the definitions in Exhibit "C" as follows:

- "Subprocessor" is equivalent to subcontractor. It is a third party who the provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its service, and who has access to Student Data.

- "Provider" is also known as third party contractor. It any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

16. To add to Exhibit "C" the following definitions:

- **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting.
- **APPR Data**: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d
- **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration, including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.
- **Disclose or Disclosure**: The intentional or unintentional communication, release, or transfer of Student Data and/or APPR Data by any means, including oral, written, or electronic.
- **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
- **Release:** Shall have the same meaning as Disclose
- **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services, then the term LEA shall also include Participating School Districts for purposes of the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.
- **Participating School District**: As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement with LEA, and shall include LEA if it uses the Services in its own educational or operational programs.

-

Exhibit "J"
LEA Documents

LEA's Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy for this service agreement can be accessed at:

https://sdpc.a4l.org/ny_dp_bor_url.php?districtID=12643

Exhibit "K"
Provider Security Policy

Provider's Data Security and Privacy Plan can be accessed at

See Attached

DELPHI RISE

INFORMATION SECURITY AND ACCOUNTABILITY PROGRAM

Date Finalized: May 15, 2023

Updated: April 23, 2025

Introduction

All information, regardless of the form or format, which is created, acquired, or used in support of Delphi Rise business activities, should only be used for Agency business. Agency Information is an asset and should be protected from its creation, through its useful life, and to its authorized disposal. It should be maintained in a secure, accurate, reliable manner and be readily available for authorized use. Information should be classified and protected based on its importance to business activities, risks, and security best practices.

Information is among Delphi Rise's most valuable assets and departments rely upon that information to support their business activities. The quality and availability of that information is essential to Delphi Rise's ability to carry out our mission. Therefore, the security of the Agency's information and of the technologies and systems that support this is the responsibility of everyone concerned. Each authorized user of the Agency's information has an obligation to protect this information in a consistent and reliable manner. Security controls provide the necessary physical, technical, and administrative safeguards to accomplish those goals.

The information within applies to all Delphi Rise Care Services (including Home Safe and information stored within the HMIS data base, Health Home Care Management Services, and Reentry services) as well as OASAS licensed programs (including Outpatient, Open Access, and Prevention services).

Expectations

1. All work computers and electronic devices issued by Delphi Rise are to be used strictly for business purposes. As a HIPAA- and 42 CFR Part 2- regulated organization, protecting sensitive client information is paramount. Personal use of work computer is prohibited to ensure compliance with confidentiality and security standards.
2. Access to Agency information technology equipment, systems, and networks where the Program Director (Information Owner) has identified the business need for limited user access or information integrity and accountability should be provided using individually assigned, unique identifiers known as Network IDs, or other technologies including biometrics, token cards, etc.
3. Individuals who use Agency information technology equipment should only access information assets to which they are authorized and for which they have a specific job-related need.
4. Individuals are not allowed to download any Protected Health Information or any other protected or sensitive information except as needed for their assigned job duties.
5. Associated with each Network ID is an authentication token such as a password which should be used to authenticate the person accessing the data, system, or network information used to authenticate the identity of a person should be treated as confidential and should mot be disclosed. This does not include distribution of on-time-use PINs, password, or passphrases.

6. Everyone is responsible to reasonably protect against unauthorized activities performed under their Network ID. This includes but is not limited to the locking of computer screens when leaving them unattended.
7. For the user's protection, and for the protection of Agency resources, **Network IDs, and passwords (or other tokens or mechanisms used to uniquely identify an individual) should not be shared.** This information should not be visibly posted or written down unless in a password protected document.

Confidentiality, Integrity, and Availability

All agency information should be protected from unauthorized access to help ensure the information's confidentiality and maintain its integrity. The information wonder should classify and secure information within their jurisdiction based on the information's value, sensitivity to disclosure, consequences of loss or compromise, and ease of recovery.

Information Security and Accountability Policy and Procedures

Included within this guide are 14 detailed policies/procedures. It is critical that staff review these policies for awareness and take responsibility for implementation.

These policies include:

1. Monitoring and Enforcement
2. Functional Role and Responsibilities
3. Electronic Resources & Data Use Policy
4. Acceptable Use Email, Mobile Devices, Office Phone, Voice over Internet Applications, Internet, Printers, and Fax-Job Aid: EPHI practices
5. Authentication and Password Management, Device Media Controls and Malicious Software
6. Information Security Risk Analysis and Risk Management
7. Assessments of Information Security and Corrective Actions
8. Workforce Access to PHI
9. Use Access Management
10. Workstation Security
11. Information Breach Response
12. Asset Disposal Policy-Appendix schedule of Asset Disposal
13. IT Support Requests Policy
14. Remote Access Policy

Title: Information Security and Accountability: Monitoring and Enforcement	**Reviewed by:** Jennifer Cathy, President, and CEO; Mary LaDuca, COO
Date Last Reviewed: April 23, 2025	**Pages: 1**

Policy:

Computer systems and resources provided by Delphi Rise are owned by the agency and are therefore its property. As such, Delphi Rise reserves the right to monitor all voice and data traffic passing through its system. This included, but is not limited to email, text and voice messages, internet use, and history.

Procedure:

1. Back-up copies of voice and data traffic may exist, despite user deletion, in compliance with Delphi Rise's records retention policy. The goal of these back-up archiving procedures is to ensure system reliability and prevent business data loss.
2. Caution should be used when communicating confidential or sensitive information via email.
3. All email messages sent outside of Delphi Rise become the property of the receiver.
4. Any allegations of misuse should be promptly reported to the Chief Operating Officer (COO). Offensive or suspicious emails should not be forwarded, deleted, or replied to. Instead, a report should be made directly to the individual named above.
5. Delphi Rise assumes no liability for the direct and/or indirect damage arising from an employee's use of Delphi Rise's voice or data services. Employees are solely responsible for the content they disseminate. Delphi Rise is not responsible for third-party claims, demand, or damage arising out of the use of the agency's voice or data services.
6. Violations of the Information Security Policy will be treated like other allegations of wrongdoing at Delphi Rise. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for inappropriate use of Agency voice or data services may include, but are not limited to, one or more of the following:

    1. Temporary or permanent revocation of access to voice or data resources.
    2. Disciplinary action according to agency policy.
    3. Termination of employment.
    4. Legal Action according to applicable laws and contractual agreements.

Title: Information Security and Accountability: Functional Role and Responsibilities	**Reviewed by:** Jennifer Cathy, President, and CEO; Mary LaDuca, COO
Date Last Reviewed: April 23, 2025	**Pages: 2**

Policy:

Each Delphi Rise department is responsible for establishing a process to assess the sensitivity of information. This process must align with industry best practices, directives from state funders, and applicable legal and regulatory requirements. The goal is to ensure that appropriate protection levels and user access are determined and applied consistently.

Program Directors and Supervisors play a critical role in upholding the Delphi Rise Information Security and Accountability Program.
Their responsibilities include:

1. Implementing Security Policies: Enforce acceptable use practices and information security guidelines within their program.
2. Promoting Security Awareness: Provide ongoing training and awareness initiatives to educate staff on information protection and proper data handling practices.
3. Monitoring Regulatory Changes: Stay informed of and respond to significant changes in legal, regulatory, or funding requirements that impact information security.
4. Incident Response Coordination: Lead or support timely responses to security incidents in accordance with agency protocols.
5. Communication Requirements: Ensure all staff and third-party partners are informed of relevant security requirements. These expectations must also be incorporated into third-party contracts and agreements.
6. Annual Staff Acknowledgment: Conduct annual reviews with staff to confirm that they have read, understood, and signed an attestation acknowledging their responsibilities under the Delphi Rise Information Security and Accountability Program. This includes confirmation of training on handling sensitive and protected health information (PHI).
7. Compliance Review and Audits: Review established security procedures and participate in internal audits in collaboration with the Compliance Officer and Compliance Committee.

The Chief Operating Officer is responsible for leading the agency's strategic direction and oversight of information security practices.
Key responsibilities include:

1. **Information Security Architecture:** Develop, implement, and maintain a comprehensive information security architecture that includes security guidelines, mechanisms, processes, standards, and procedures aligned with current and future business needs.
2. **Security Risk Guidance:** Provide strategic guidance to departments on emerging security threats that could impact agency operations and IT infrastructure. Recommend and support the implementation of tools and procedures to mitigate associated risks.
3. **Departmental Security Support:** Assist department directors and supervisors in implementing additional security measures tailored to their specific operational needs.

4. **Training and Awareness:** Oversee the development and delivery of ongoing security training and awareness initiatives to ensure all users, including employees, contractors, consultants, vendors, interns, and volunteers, understand and comply with the agency's security requirements.
5. **Incident Investigation and Response:** Investigate security breaches and report findings to senior management. Where necessary, put additional safeguards in place to prevent similar issues and protect agency systems and data.

<u>All Agency Employees:</u>

1. It is the responsibility of all employees to protect the agency's information and resources, including passwords.
2. To report suspected security incidents to one of the following: a supervisor, the Human Resource Administrator, the Compliance Officer/COO, or the CEO.
3. Adhere to the guidelines outline in *Delphi Rise's Information Security and Accountability Program and Corporate Compliance Program.*

Note: All individuals working with or on behalf of Delphi Rise, including contractors, consultants, vendors, interns, volunteers, and others in similar roles are also required to protect agency information and resources. They must comply with all applicable policies within the *Information Security and Accountability Program* and the *Corporate Compliance Program*.

Title: Information Security and Accountability: Electronic Resources & Data Use Policy	**Reviewed by:** Jennifer Cathy, President, and CEO; Mary LaDuca, COO
Date Last Reviewed: April 23, 2025	**Pages: 2**

Policy:

Delphi Rise provides a range of electronic resources to support business operations. These resources include, but are not limited to, laptops, tablets, smartphones, local and wide area networks, software, internet, and email services. Use of these tools, and the protection of all sensitive or protected data—regardless of format (electronic, paper, text, or voice), must be guided by sound judgment, professionalism, and compliance with agency standards. The purpose of this policy is to define the acceptable limits within which users may exercise their discretion.

Procedures:

1. No Expectation of Privacy: All agency-owned electronic resources are the property of Delphi Rise and are intended for official business use. Users should have no expectation of privacy. The agency reserves the right to monitor and inspect internet use, emails, and all technology activities. Monitoring tools and software may be used. Use of Delphi Rise systems constitutes consent to such monitoring without prior notice.
2. Prohibited Personal Use: Agency technology and electronic resources are provided strictly for work-related activities. While occasional minimal personal use (such as checking a personal email or confirming an appointment) may be tolerated, employees must not misuse agency resources for non-business purposes. This includes, but is not limited to:
    - Streaming videos or music for personal entertainment during work hours
    - Using agency computers or networks for online shopping, gaming, or social media scrolling unrelated to work
    - Sending mass personal emails or texts from agency devices
    - Engaging in personal business ventures, such as running side businesses, marketing products, or handling personal finances
    - Sharing or promoting personal, religious, or political views through agency platforms or email
    - Visiting inappropriate or non-work-related websites, including those related to gambling, adult content, or other prohibited content
    - Downloading unauthorized software, apps, or media files for personal use

    Such use may compromise system security, reduce productivity, and put protected data at risk. Misuse of agency resources can result in disciplinary action, up to and including termination.

3. Data Ownership and Storage: All data, records, software, and information stored or created on agency systems are the property of Delphi Rise. Users must save work to designated departmental network servers rather than local device drives to ensure data security, proper backups, and accessibility.
4. Email and Account Use: Agency-provided email addresses must be used for all official correspondence. Sharing email accounts or passwords, or attempting to access another person's account, is strictly prohibited. Each user is responsible for the use of their assigned account and credentials.

5. Password Security: If a user suspects their password has been compromised, they must change it immediately and report the incident to their supervisor or IT support. Prompt reporting helps protect agency systems from unauthorized access.
6. Policy Violations: Any violation of this policy may result in disciplinary action, up to and including termination, and may also lead to criminal prosecution where applicable.

Title: Information Security and Accountability: Acceptable Use and Security Policy for Communication and Office Technology Resources *(Covers Email, Mobile Devices, Office Phones, VoIP, Internet, Printers, and Fax Systems)*	**Reviewed by:** Jennifer Cathy, President, and CEO; Mary LaDuca, COO
Date Last Reviewed: April 23, 2024	**Pages: 4**

Policy:

Delphi Rise's Acceptable Use Policies define appropriate and prohibited behaviors related to the use of these systems. The goal is to protect sensitive information, ensure the reliability and security of systems, maintain operational efficiency, and comply with all relevant healthcare regulations and organizational policies.

The organization reserves the right to monitor the use of telephones, voicemail, text messages, mobile devices, VoIP systems, printers, and fax machines. This includes the ability to review voicemail content and, when warranted, telephone conversations.

Monitoring telephone, text, and voicemail use will only be conducted for legitimate business purposes. These purposes may include assessing customer service and quality assurance, verifying staff compliance with organizational policies, retrieving lost messages, recovering from system failures, supporting internal investigations, responding to allegations of misconduct or wrongful acts, and fulfilling legal or regulatory obligations.

<u>Acceptable Use: Office Telephones</u>

1. All telephones, telephony equipment, voicemail boxes, and messages, including text contained within voicemail boxes are the property of Delphi Rise.
2. Program directors or their assigned designee are responsible for overseeing telephone and voicemail use and ensuring policy compliance, as well as ensuring the Chief Operating Officer (COO) is notified of any additions, moves, or changes required to telephone and voicemail services.
3. Voicemail boxes will be protected with a PIN (personal identification number). PINs must not be shared with others.
4. A standard recorded script for the outgoing greeting is used by all Delphi Rise employees.
5. Employees are expected to check their voicemail daily. If they are unable to do so, they must enable the out-of-office greeting to reflect their unavailability and, if applicable, provide alternate contact information to ensure uninterrupted communication.

<u>Acceptable Use: Email</u>

1. The standard email form includes Delphi Rises' Confidential Notice as the closure of every agency email correspondence.
   "CONFIDENTIALITY WARNING This message is intended only for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential, and exempt from disclosure under applicable law. If the reader of the message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of the communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone (585-467-2230) and destroy the original message."

2. **Signatures:** The standard format for email signatures at Delphi Rise shall include the following information: name, job title, department, address, phone number, fax number, preferred pronouns, and email address. A signature is required for both internal and external emails. Only business-related content, including the organization's approved mission statement, may be included in email signatures. Personal slogans, beliefs, or extraneous messages are not permitted, unless specifically authorized by the Chief Operating Officer (COO) or CEO.
3. **Email Management:** Users are responsible for managing their email inboxes, including organization and regular cleanup. Emails containing Protected Health Information (PHI) must be deleted from both the inbox and sent items immediately after the information has been documented in the client's electronic health record. The Deleted Items folder must be emptied regularly, as email cannot be stored there. Only open attachments from known and trusted senders. Exercise caution with emails from external sources and carefully verify the sender's email address to ensure it originates from a legitimate and recognized source.
4. If you open an attachment or link that appears suspicious or malicious in any way, you must immediately report it to Brite, our IT support team, at help@brite.com or 1-866-224-6698. They will scan your computer for any viruses or security issues to ensure your account remains secure. Brite will also assist you in changing your password to maintain ongoing security.
5. Delphi Rise's email systems and services should not be used in ways that could overload or strain the system. Your email use should not disrupt or affect other users' ability to access or use the email system. All email activities must follow applicable laws, agency policies, and any contracts in place. Users are expected to maintain professionalism and courtesy in both work-related and personal email communication.
6. **Forwarding:** Employees must exercise caution when forwarding any email from Delphi Rise to an external network. Unless approved by the Chief Operating Officer (COO), Delphi Rise emails cannot be automatically forwarded to external destinations. Sensitive information, or any information considered confidential, must not be forwarded through any means unless it is critical to business operations and has been properly encrypted in accordance with the guidelines outlined below.
7. **Encryption:** All employees of Delphi Rise are required to use encryption when sending emails that contain Protected Health Information (PHI) to recipients outside the Delphi Rise network. This is a critical safeguard to ensure compliance with HIPAA and other data privacy regulations. Encryption must be used consistently to protect sensitive client information from unauthorized access, interception, or disclosure. Employees should follow the organization's approved procedures and tools for secure email transmission. If there is any uncertainty about how to encrypt an email, staff must contact IT support before sending.
8. **Archiving:** Delphi Rise is committed to maintaining compliance with all legal, regulatory, and operational requirements related to email retention. As part of this commitment, certain emails including those related to client care, business operations, or legal matters must be retained in accordance with Delphi Rise's data retention policy.
   While employees are expected to delete emails containing Protected Health Information (PHI) from their inbox and sent items after the information has been properly documented in the client's electronic health record, these emails may still be retained automatically through secure archiving systems managed by the agency. Employees should not manually archive or store PHI outside approved systems.
9. **Retention of Business Records:** Any email message deemed a "business record" must be retained for the duration required by applicable laws, regulations, and Delphi Rise's retention policy. A business record is defined

as any electronic or printed document created or maintained in the ordinary course of business that has evidentiary, legal, operational, or reference value.
Not all email messages qualify as business records. However, an email—and any attachments—should be retained if it documents a business activity, is the sole copy of critical information, or holds long-term value.

10. **Litigation Hold:** If litigation is filed or reasonably anticipated against Delphi Rise or its employees, the agency is legally required to preserve all documents and records relevant to the matter. This includes emails and any related attachments. In such cases, the CEO will issue a litigation hold, notifying the appropriate individuals and providing clear instructions on which documents must be retained and how they should be preserved.
A litigation hold takes precedence over all standard email retention or deletion policies. Once a litigation hold is in place, affected employees must not delete, alter, or dispose of any potentially relevant emails or records until they are formally released from the hold.

Acceptable Use: Printers

1. All documents, including those containing Protected Health Information (PHI), must be printed using the **secure print feature** available on all Delphi Rise copiers. This feature ensures that documents are only released when the user is physically present at the printer and authenticated with a user passcode.
2. Any printed document containing PHI or other sensitive information must not be left unattended at the printer and must be retrieved promptly. When no longer needed, such documents must be disposed of securely by placing them in a designated shred bin. Under no circumstances should they be discarded in regular trash or recycling bins.

Acceptable Use: Mobile Devices

1. **Access and Network Connection**: Delphi Rise reserves the right to restrict mobile devices' access to the agency infrastructure if it is determined that such devices pose a risk to the agency's systems, data, or users. The COO will oversee any such actions.
2. **Network and Data Access**: Laptop computers may only connect to the agency network via Secure Socket Layer (SSL) and Virtual Private Network (VPN) connections. The SSL VPN portal address will be provided as needed.
3. **Personal Devices**: Personal mobile devices, including smartphones, are not allowed to access the agency network or email. Senior leadership is permitted to use mobile devices for this purpose. All other exceptions must be formally approved through the Access Exception Form process and authorized by senior leadership. For staff who are approved to use their personal mobile devices for work email, the following reimbursement structure will apply:
    - $20.00 per pay period
    - Reimbursement will be included as part of the normal bi-weekly payroll processing
4. **Security Measures and Loss Reporting**: All mobile device users must implement reasonable security measures (e.g., passwords, encryption, device control) to protect sensitive data. In the event of a lost, stolen, or damaged device, users must report it to their supervisor immediately. The device will be remotely wiped and locked. If recovered, it can be submitted to IT for reprovisioning. Loss due to negligence may result in the employee being responsible for replacement costs.

5. **Acquisition and Use**: All mobile services, including cell phones and mobile broadband devices, must be acquired through the COO following standard agency procurement procedures. Agency-issued devices are to be used solely for authorized business purposes and should not be used excessively or in ways that hinder productivity.
6. **Mobile Device Care and Safe Use**: Employees are responsible for properly caring for agency-issued mobile devices to prevent damage, loss, or theft. Additionally, employees are prohibited from using mobile devices while operating agency or personal vehicles, heavy machinery, or equipment to ensure safety.

Acceptable Use: Voice or Video-over Internet Protocol (VoIP) and other Internet Access and Use

1. **Access and Approval:** All services such as Vonage, Doxy.me, and Zoom must be requested through the Chief Operating Officer (COO) and follow standard Delphi Rise procurement procedures. Staff should not independently purchase or create accounts for these platforms.
2. **Authorized and Appropriate Use:** Only Delphi Rise staff and individuals authorized to conduct agency business may use agency-provided access to VoIP or video communication tools, including Vonage, Zoom, and Doxy.me. These tools are to be used for business purposes only. Personal use, or any use that is excessive, disrupts productivity, or interferes with others' ability to work, is not permitted.
3. **Approved Services Only:** Employees must only use Delphi Rise-approved platforms for voice or video communication. Unauthorized applications or services may not be used to conduct agency business.
4. **Internet Monitoring and Responsible Use:** All internet activity on Delphi Rise equipment or accounts may be monitored. Internet access is filtered using security software to restrict access to non-business-related or inappropriate sites. Staff are expected to use the internet responsibly, exercising sound judgment and discretion at all times. Any internet use that violates laws or agency policies may be reviewed and documented for further action in accordance with due process.
5. **Telehealth Security and Consent:** OASAS program employees conducting telehealth sessions using VoIP must obtain written consent from the client prior to the session. A copy of the signed consent must be included in the client's clinical record. Staff must also follow all required security protocols to protect client health information and ensure a safe and confidential telehealth experience.

Title: Information Security and Accountability: Authentication and Password Management, Device Media Controls and Malicious Software	**Reviewed by:** Jennifer Cathy, President, and CEO; Mary LaDuca, COO
Date Last Reviewed: April 23, 2025	**Pages: 1**

Policy:

The purpose of this policy is to establish guidelines for creating, managing, and protecting passwords to safeguard access to Delphi Rise information systems, including systems that store electronic Protected Health Information (ePHI) and other sensitive data. This policy applies to all Delphi Rise employees, contractors, consultants, vendors, interns, volunteers, and others in similar roles.

Employees must create strong, unique passwords to authenticate their access to these systems. Passwords should be kept secure, confidential, and never shared with others. Staff are expected to use these passwords responsibly to protect sensitive information and prevent unauthorized access.

In addition, under no circumstances should portable devices such as USB memory sticks, flash drives, external storage devices, or other removable media be connected to the network. This restriction also applies to any hardware or devices that facilitate connectivity to USB-based storage through wired or wireless methods, such as Wi-Fi, Bluetooth, or other wireless technologies. This measure is designed to prevent unauthorized data access or transfer.

Delphi Rise is committed to maintaining a secure environment. To that end, all workstations must have up-to-date anti-virus software installed. The system will be configured to automatically activate and update the anti-virus software to ensure protection against malicious software and threats.

Procedure:

1. Each user account consists of a unique user ID and password that allows Delphi Rise to hold users accountable for their activities on the network. Users must not share their password with anyone and will be held responsible for activities associated with their account.
2. If a user is locked out or cannot remember their password for access to the Delphi Rise network, they can call Brite at 1-866-224-6698 requesting that their password be reset. The Program Director or their designee are responsible for communicating to their users any requirements for establishing and maintaining passwords for password-protected applications used within their department.
3. Files from unknown or suspicious sources shall not be downloaded.
4. Protected information should never be stored on a portable storage device.
5. Users MUST save their data to the appropriate secure network drive (home folder or shared folder) so that all data is backed up regularly and can be recovered if needed.
6. If a virus, worm, or other malicious code has infected or been identified on a server or workstation that poses a significant risk that equipment shall be disconnected from the network until it has been appropriately cleaned.
7. Disabling automatic virus scanning features is prohibited.
8. Only agency owned or COO approved devices may connect to the agency network using VPN.
9. Brite should be contacted immediately if a virus is suspected.

Title: Information Security and Accountability: Information Security Risk Analysis and Risk Management	**Reviewed by:** Jennifer Cathy, President, and CEO and Mary LaDuca, COO
Date Last Reviewed: April 23, 2025	**Pages: 1**

Policy:

Delphi Rise shall perform information security risk analysis and management through periodic audits, risk assessments and implementation of security access controls to mitigate risks. Information system activity reviews and audits may be conducted to ensure integrity, confidentiality, and availability of information and resources.

Procedure:

The following activities are required to ensure risk is mitigated:

1. Periodic program assessment including a security review of facility access and controls, document destruction, and protection of network/sever closets, workstations, and portable devices.
2. Assessments of new or existing information system applications that contain or are used to protect EPHI and other protected information.
3. Assessment of new programs, departments, or changes in the mode of manner of service delivery involving EPHI and other protected information.
4. Workforce security training and awareness reminders.
5. Manage changing controls with Brite and The Ten Eleven Group for all alterations that occur in the information systems that support, contain, or protect EPHI. This includes the installation, update, or removal, of network, services and components, and operating system upgrades.
6. Implement a mechanism to record all failed log-in attempts on network systems containing EPHI when the technology is capable. To the extent that technology allows, a means to disable any User ID that has more than three consecutive failed log-in attempts within a 30-minute period.
7. Undergo a review of log-in activity reports and logs when required to identify any patterns of suspicious activity, such as continuous failed log-in attempts as well as gold up investigations of possible security incidents to ensure compliance.
8. Verify the updates are maintained at the appropriate security level. Verify that virus protection is current.

Title: Information Security and Accountability: Information Security Assessments and Corrective Action	**Reviewed by:** Jennifer Cathy, President, and CEO and Mary LaDuca, COO
Date Last Reviewed: April 23, 2025	**Pages: 1**

Policy:

The Privacy Officer will make periodic visits to each Delphi Rise Program area to observe that information security safeguards are adequate.

Procedures:

The Privacy Officer will conduct assessments of program areas using a standard tool (*Figure A*) and provide comments and recommendations to Delphi Rise senior leadership and Compliance Committee. Opportunities for improvement will be documented in the assessment by the Privacy Officer. The responsible department will be required to implement and document improved compliance with information security safeguards.

Figure A

Department Area	**Date of Review**	**Yes/No/NA**
Restricted areas and/or files are locked		
Public access is limited at workstations		
Prescence of shredders and/or blue recycling containers		
Shredders and/or blue recycling containers easily accessible		
No conversation in public areas in private locations		
Private telephone conversations are in private locations		
No staff having confidential conversations in non-private areas (elevators, hallways, etc.)		
No Papers with PHI in areas where it can be viewed by others		
No PHI in discard or trash		
PHI in offices is locked in desk or cabinet		
Computer screens are shielded or located in a manner that prevents access by unauthorized personnel		
Programs with PHI are exited, and the employee is logged off when computer is left unattended		
Email messages contain a confidentiality statement		
Screen Lock on computers is set		
Print Jobs are sent using private print		
Senior Leadership Comments and Recommendations: Corrective Action:		Date: Date:

Title: Information Security and Accountability: Workforce Access to PHI	**Reviewed by:** Jennifer Cathy, President, and CEO and Mary LaDuca, COO
Date Last Reviewed: April 23, 2024	**Pages: 1**

Policy:

Delphi Rise has established access control policies for its computing network, applications, workstations, and any areas where hardcopy or electronic Protected Health Information (PHI) is stored or accessed. As a covered entity under the HIPAA Privacy Rule, Delphi Rise ensures that only workforce members with a legitimate work-related need are granted access to PHI, including electronic and paper records containing personal, financial, and identifiable health information.

Procedure:

1. Only the workforce members' Program Director or an assigned designee can authorize access to the Delphi Rise information systems. This will be done using *Delphi Rise Employee Hire/Change Form.*
2. If the workforce members' need for access changes, due to changes in job duties or termination, it is the responsibility of the Program Director or their designee to authorize the change or termination of access by completing the *Delphi Rise Employee Hire/Change Form*.
3. Access to the information system or application may be revoked or suspended, consistent with Delphi Rise policies and practice, if there is evidence that an individual is missing information or other resources. Any individual whose access is revoked or suspended may be subject to disciplinary action or other appropriate corrective measure.
4. Each Program Director or their designee is responsible for ensuring that the access to EPHI and other sensitive information and protected information granted to the workforce member is the minimum, necessary access required for each work role and responsibilities.
5. Any client or staff member who wishes to block a user or users from access to sensitive information will notify the Chief Operating Officer. User access controls are capable of blocking access to sensitive client information by employee name or by program. User access can be limited to billing, front end, and senior management staff only, if need be. If an employee has previously utilized services at Delphi Rise, their chart is blocked from all program staff and access is limited to billing staff.

Title: Information Security and Accountability: User Access Management	**Reviewed by:** Jennifer Cathy, President, and CEO and Mary LaDuca, COO;
Date Last Reviewed: April 23, 2024	**Pages: 1**

Policy:

Each department's program director or their designee is responsible for verifying that a workforce member's access to PHI and other sensitive information is appropriate. They must determine and request the necessary systems and access levels based on the individual's job responsibilities.

Procedure:

1. Prior to being issued a User ID or logon account to access any PHI or other sensitive and protected information each workforce member shall read and sign an attestation that they have read and agree to comply with *Corporate Compliance Plan* and The Information *Security and Accountability Program Policies.*
2. The Program Director or their designer shall document that each workforce member is trained on the topics listed below. This shall occur at on-boarding and annually as a refresher for all departments that handle PHI or other sensitive and protected information. In-service type or e-learning, for departmentally specific applications will occur on a regular basis. This can include but is not limited to:
    1) Proper use and of disclosure of PHI or other sensitive and protected information stored in the systems and/or application.
    2) Proper log-on and log-off procedures
    3) Protocols for correcting user errors
    4) Instructions on contacting a designated person or help desk when PHI or other sensitive and protected information may have been altered or destroyed in error
    5) Reporting a potential or actual security breach
3. System administrators will only process access requests that have been authorized by Program Directors or their designee utilizing the *Employee Hire/Change Form.*
4. The COO has the authority to grant emergency access for workforce members who have not completed the normal HIPAA access requirements in an emergency or in response to a natural disaster.
5. Program Directors or designee are responsible for making the necessary arrangement for changing or removing a workforce member's access to EPHI and other sensitive and protect information. If sensitive information is input and stored in third party/external/vendor programs or databases, they will follow those specific protocols for removing or changing access to all systems.
6. To protect agency information from malicious intent or unauthorize use by non-employees, each Program Director or designee is responsible to report a terminations of employment (voluntary and non-voluntary), employee suspensions, or employee leave anticipated to be for more than four weeks (e.g., medical, worker's comp) to the COO within 24 hours, using the *Employee Hire/Change Form*. In an urgent situation, immediate notification to the COO by phone is required.

Title: Information Security and Accountability: User Access Management	**Reviewed by:** Jennifer Cathy, President, and CEO and Mary LaDuca, COO
Date Last Reviewed: April 23, 2025	**Pages: 1**

Policy:

Delphi Rise shall implement safeguards to prevent unauthorized access to PHI through workstations and to protect PHI from any intentional or unintentional use or disclosure. Since PHI can be portable, this policy requires workforce members to protect EPHI at Delphi Rise worksites and all other locations including remote work.

Procedure:

1. All workstation computers used by workforce members with access to EPHI must be configured to automatically lock after 10 minutes of inactivity, requiring a password to unlock. Workforce members are also required to manually lock their workstations using the Ctrl+Alt+Delete key combination whenever the computer is left unattended.
2. Workforce members shall ensure that observable confidential information is adequately shielded from unauthorized disclosure and access on computer screens. At each site, every effort shall be made to ensure that confidential information on computer screens is not visible to unauthorized persons.
3. Workforce members who work from home or other non-office sites shall follow the above workstation security controls to safeguard EPHI access or viewing by any unauthorized individual.
4. Workforce members shall protect printed versions of EPHI that have been transmitted via fax or multi-use machines by promptly removing documents from shared devices.
5. Whenever possible, confidential documents are to be placed in locked cabinets or drawers when left unattended.

Title: Information Security and Accountability: Information Breach Response	**Reviewed by:** Jennifer Cathy, President, and CEO and Mary LaDuca, COO
Date Last Reviewed: April 23, 2025	**Pages: 3**

Policy:

Delphi Rise will respond to all impermissible uses or disclosures of protected or private information. A breach will be presumed unless Delphi Rise or its business associate, as applicable, demonstrates through a documented risk assessment that there is a low probability that the information has been compromised. All incidents involving impermissible use, disclosure, or breaches of electronic or hardcopy protected or private information must be promptly reported and addressed.

Procedure:

Workforce members shall immediately notify their supervisor of any suspected or confirmed breach or disclosure incident. They in turn will notify one of the following: the Human Resource Administrator; the Compliance Officer the; the Privacy Officer; or the CEO, who will evaluate the situation to determine the appropriate response to the report disclosure or breach incident and initiate the process as required by the type of incident.

The Compliance Officer and CEO WITHOUT UNREASONABLE DELAY shall:

1. Perform and document a risk assessment based on the disclosure/breach identified: the process to be followed is assessing the risk of harm to the individual. Delphi Rise and business associates must assess the probability that the protected health information has been compromised based on a risk assessment that considers at least the following factors:
    a) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification. This must include a "sensitive rating." For example, with respect to financial information this included credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud. In such cases, other laws may apply.
    b) The unauthorized person who used the protected health information or to whom the disclosure was made. Whether the protected health information has been mitigated.

Following a breach or suspected breach of suspected breach of unsecured protected health information, Delphi Rise shall:

1. Provide a notice of breach to prominent media outlets serving a state jurisdiction, following the discovery of a breach if the PHI of more than 500 residents of such state or jurisdiction, is reasonably believed to have been accessed, acquired, or disclosed during such breach. This notice is in addition to, not a substitute to, the required written notices, and shall be provided in the following form:
    a) Written notification by first-class mail to the individual at their last known address or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by email. Notification may be provided in one or more mailings as more information becomes available.
    b) In cases where the individual is known to be deceased, the next of kin or personal representative of the individual will be contacted if that address is available (as specified under §164.502(g)(4) of subpart E, *written notification by first-class mail to either the next of kin or personal representative of the individual.*

c) Substitute notice. In the case where there is insufficient or out-of-date contact information that precludes written notification to the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual.
d) In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then substitute notice may be provided by an alternative form of written notice, telephone, or other means.
e) In the case in the in which there is insufficient or out-of-date contact information for 10 conspicuous posting for a period of 90 days on the home page of Delphi Rise's web site, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely residue. In addition, there must be a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's secured protected health information may be included in the breach.
f) In the case deemed by Delphi Rise to require urgency because of possible imminent misuse of unsecured protected health information, Delphi Rise may provide information to individuals by telephone or other means, as appropriate, in addition to written notice.
g) Inform prominent media outlets serving the State or jurisdiction.

2. Except as provided in §164.412, Delphi Rise shall provide the notification required without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
3. The content of the notification required shall meet the requirements of §164.404(c) and shall include to the extent possible:
    a) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if know
    b) A description of the PHI involved (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code)
    c) Recommend next steps the impacted individual should take to protect themselves from potential harm resulting from the breach.
    d) A brief description of Delphi Rise's actions to investigate the breach, to mitigate harm to individuals, and to protect against subsequent breaches.
    e) Contact procedures for individuals interested in learning additional information including a toll-free number, an email address, website, or postal address.
    f) The notification shall be written in plain language.

Following the discovery and subsequent risk assessment of a breach of unsecured protected health information as provided in *§164.405(a)(2)*, Delphi Rise shall:

1. Notify the Secretary of Health and Human Services
2. For breaches of unsecured protected health information involving 500 or more individuals, provide the notification required in the manner specified on the HHS website at: https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true
3. For breaches of unsecured protected health information involving less than 500 individuals, Delphi Rise shall maintain a log or other documentation of such breaches. In a period not to exceed 60 days after the close of the

calendar year, Delphi Rise will provide notification required for those breaches occurring during the preceding calendar year in a manner specified on the HHS website at: https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true

4. Delphi Rise is required to notify all individuals when there has been or is reasonably believed to have been an unintended disclosure or compromise of the individual's private information (PII, PHR, PHI, etc.) in compliance with the applicable *Information Security Breach and Notification Act* affecting Delphi Rise and this policy.
5. Other than the above requirements for reporting to external agencies, all impermissible use, breach, or disclosure related incidents and their outcomes, and communications documented. That documentation will be saved for at least seven years or as needed to meet any claims, legal challenges, or other compliance activities.
6. Each calendar year, the log will be reviewed, and disclosure will be reported to the Board of Directors by the Compliance Officer.

Title: Information Security and Accountability: Asset Disposal	**Reviewed by:** Jennifer Cathy, President, and CEO and Mary LaDuca, COO
Date Last Reviewed: April 23, 2025	**Pages: 1**

Policy:

Delphi Rise has established and defined standards, procedures, and restrictions for the disposal of non-leased IT equipment in a legal, cost-effective manner. Delphi Rise's surplus or obsolete IT assets and resources (i.e., desktop computer, servers, cell phones etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents. Therefore, all disposal procedures for retired IT assets must adhere to agency approved methods.

Procedure:

1. To ensure the proper tracking of Delphi Rise's computer resources and its correct status, the Office Manager maintains an up-to-date asset inventory within Human Resources.
2. Disposal and disposal procedure of all IT assets and equipment will be centrally managed and coordinated by Delhi Rise's Senior management. The Chief Operating Officer (COO) overseas selecting and approving external agents for recycling hardware and/or sanitizing hardware of harmful toxins before shipment to landfills. The Chief Operating Officer (COO) is also responsible for acquiring credible documentation from third parties that are contracted to conduct the data wiping, tag or label removal, or any other part of the disposal process.

Acceptable methods for the disposal of IT assets are as follows:

1. Reassigned to a less critical business operation function.
2. Recycled by a licensed and approved service provider in accordance with all local, state, and federal laws, who by contract agrees to wipe or to shred all data storage devices.
3. A log should be maintained of all media that have been disposed. The log should include the date, type of device, manufacturer, serial number (if one exists), sanitation or destruction method used, disposal method (e.g., sold or recycled).

Title: Information Security and Accountability: IT Support Requests	**Reviewed by:** Jennifer Cathy, President, and CEO and Mary LaDuca, COO
Date Last Reviewed: April 23, 2025	**Pages: 1**

Policy:

Delphi Rise employees will initiate a support request to the IT vendor for application or infrastructure concerns. Phone calls to the Chief Operating Officer (COO) should be limited to large-scale issues such as a suspected virus or breach while disrupts services for multiple users or interrupts a critical function.

Procedure:

1. All requests for access rights including but not limited to user accounts, access to file shared and/or password protected applications should be directed to the Chief Operating Officer (COO) by the Program Director or an assigned designee, using the appropriate template.
2. All non-urgent support requests for problems with applications, networking or hardware should be entered by sending an email to help@Brite.com. Urgent requests can be initiated by calling 1-866-224-6698.
3. Departments may choose to direct their staff to identify department members to initiate requests on behalf of others. This policy applies to all local and remote employees, management, individuals such as contractors, consultants, vendors, interns, volunteers, and other persons in similar positions, and any other parties who rely on access to Delphi Rise resources. While all approved moves, additions, and/or changes will be carried out in as timely a manner as possible, they may be delayed in the event of an IT-related problem or emergency.

Title: Information Security and Accountability: Remote Access Policy	**Reviewed by:** Jennifer Cathy, President, and CEO and Mary LaDuca, COO
Date Last Reviewed: April 23, 2025	**Pages: 2**

Scope:

Delphi Rise employees and individuals who work under agreement with Delphi Rise (e.g. contractors, consultants, vendors, interns, volunteers, and other persons in similar positions) via a remote access connection OF ANY KIND, is covered by this policy. Work can include but is not limited to email correspondence, web browsing, utilizing intranet resources, and any other agency application used over the internet. Remote access is defined as any connection in the agency's network and/or other application from non-Delphi Rise networks, such as employee's home, a hotel room, airports, cafes, satellite office, wireless devices, etc.

Policy:

All remote access and mobile privileges to Delphi Rise network and resources- and for wireless Internet access via hotspots- must employ only Delphi Rise-approved methods. Remote access to Delphi Rise networks and resources is for Delphi Rise business purposes only. It is imperative that any remote access connection is used to conduct Delphi Rise business be utilized appropriately, responsibly, and ethically.

Procedures:

1. Employment at Delphi Rise does not automatically entitle workforce members to remote access to the organization's network and resources. Remote access may be granted only after the proper encryption technology and strong password authentication measures are installed. Once access is approved, users are responsible for maintaining and using the remote access tools in compliance with Delphi Rise's remote access policies and procedures. Failure to adhere to these policies may result in suspension or termination of remote access privileges and/or other disciplinary actions.
2. Requests for remote access to Delphi Rise network and resources will be initiated by the employees' Program Director or designee using the *Employee Hire/Status Change Form.*
3. All remote access privileges will be centrally managed by the Delphi Rise Chief Operating Officer.
4. Employees will use secure remote access procedures. This will be enforced through public/private key encrypted strong password in accordance with Delphi Rise' password policy. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.
5. All remote computer equipment and devices used for business interest, whether personal or agency-owned, must be physically secure. If a personal or agency-owned computer or related equipment used for remote access is damaged, lost or stolen, the authorized user will be responsible for notifying their manager and Delphi Rise's Chief Operating Officer immediately.
6. Devices used to access the Delphi Rise network will have antivirus software. The user is responsible to periodically connect to the network on site to update antivirus and other software updates.
7. Remote users must connect their devices using Delphi Rise's approved personal firewall, (i.e., VPN "GlobalProtect") and any other security measure deemed necessary. VPNs supplied by the wireless service

8. provider “hot spot” should also be used, but only in conjunction with Delphi Rise’s additional security measures. Public, unsecured internet connections are prohibited.
9. Employees, contractors, and temporary staff with remote access privileges must ensure that their computers are not connected to any other network. While connected to Delphi Rise’s network via remote access, with the obvious exception of internet connectivity.
10. The remote access user also agrees to immediately report to their Program Director or assigned designee and the Chief Operating Officer (COO) any incident or suspected incident of unauthorized access and/or disclosure of Agency resources, databases, networks, etc.
11. The remote access user also agrees to and accepts that his or her access and/or connection to Delphi Rise’s networks may be monitored to record dates, times, duration of access, etc., to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done to identify accounts/computers that may have been compromised by external parties.

jennifer cathy dated: 6/17/2025

DelphiRise_WebsterCentral_NYonly_VendorSigned

Final Audit Report 2025-09-02

Created:	2025-09-02
By:	TEC SDPA (mklisiwecz@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAACQqwpI6BnFW3aPnfQitU3kFloWBgM2LV

"DelphiRise_WebsterCentral_NYonly_VendorSigned" History

Document created by TEC SDPA (mklisiwecz@tec-coop.org)
2025-09-02 - 2:56:11 PM GMT

Document emailed to Brian Zimmer (brian_zimmer@webstercsd.org) for signature
2025-09-02 - 2:56:18 PM GMT

Email viewed by Brian Zimmer (brian_zimmer@webstercsd.org)
2025-09-02 - 3:07:02 PM GMT

Document e-signed by Brian Zimmer (brian_zimmer@webstercsd.org)
Signature Date: 2025-09-02 - 3:07:41 PM GMT - Time Source: server

Agreement completed.
2025-09-02 - 3:07:41 PM GMT