Embrace504® Contract

Embrace®
PO Box 305
Highland, IL 62249

The Board of Trustees of Illinois State University
100 North University Street
Normal, IL 61790

The following is an Embrace504® Contract (hereinafter “contract” or “agreement”) for software, website hosting, and support services. This contract is made between Brecht’s Database Solutions, Inc. d/b/a Embrace® (hereinafter “Embrace®”, “We”, “Us” or “Licensor”) and The Board of Trustees of Illinois State University (hereinafter “You”, “Your” or “Licensee”).

EMBRACE®
Embrace504®
WEBSITE LICENSE AGREEMENT

NOTICE TO USER: PLEASE READ THIS AGREEMENT CAREFULLY. BY USING ALL OR ANY PORTION OF THE WEBSITE YOU ACCEPT ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT.

YOU AGREE THAT THIS AGREEMENT IS LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU. THIS AGREEMENT IS ENFORCEABLE AGAINST YOU AND ANY LEGAL ENTITY THAT OBTAINS ACCESS THROUGH LICENSEE TO THE WEBSITE AND ON WHOSE BEHALF IT IS USED. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT EXECUTE THIS CONTRACT OR USE ANY OF OUR PRODUCTS OR WEBSITE.

Embrace® owns all intellectual property in/on the Embrace® website (hereafter “website”) and its related Embrace® software (hereafter “software”). Embrace® agrees to allow you and/or your authorized agents to login and access the website and use our software only in accordance with the terms of this Agreement. Any unauthorized access or use of Embrace’s products is cause for immediate termination of your access to its products by all means available to us.

1. LICENSE TO ACCESS WEBSITE. As long as you obtained access to the website from Embrace® and as long as you comply with the terms of this and any other Agreement you have with Embrace®, Embrace® grants you a non-exclusive license to use the website in the manner and for the term and purposes described below.

2. INTELLECTUAL PROPERTY OWNERSHIP. The website and its related software are the intellectual property of and are owned by Embrace®. The structure, organization, and code of the website and its related software contain valuable trade secrets and confidential information of Embrace®. Except as expressly stated herein, this Agreement does not grant you any intellectual property rights whatsoever in the website and its related software and all rights are reserved by Embrace®.

Any form, database, or software that is altered, conceived, made, or developed in whole or in part by Embrace® (including any developed jointly with you) during or as a result of our relationship with you shall become and remain the sole and exclusive property of Embrace®. You agree to make no claim in the rights or ownership of any such form, database or software.

To the extent that any custom form is created by Embrace® for you, based upon any prior form, template or exemplar provided by you, you warrant and represent to Embrace® that you created said form(s) or have the legal right to use said form(s). You agree to indemnify Embrace® for any third-party claims for infringement, misappropriation or other violation of any third-party’s intellectual property rights where such claims are made against Embrace® for forms, templates or exemplars created based upon material provided by you to Embrace®.

3. DATA SECURITY. Embrace’s database or software may host privacy protected data provided by you concerning students and employees. This information is privacy protected by federal and state law, including the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g)(“FERPA”), the Illinois School Student Record Act (105 ILCS 10/), the Personnel Record Review Act (820 ILCS 40/) and the Student Online Personal Protection Act (105 ILCS 85/1 et seq.)(“SOPPA”).

Embrace will store and process Data in accordance with industry best practices. This includes appropriate administrative, physical, and technical safeguards to secure Data from unauthorized access, disclosure, and use. Provider will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. Provider will also have a written incident response plan, which will include prompt notification of the School District in the event of a security or privacy incident, as well as best practices for responding to a breach of Personally Identifiable Information (“PII”). PII shall include, but is not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by District or its users, students, or students' parents/guardians.

Embrace® acknowledges that all of your data uploaded, stored, or otherwise coming into contact with Embrace’s database or software, is and shall remain your sole and exclusive property and be subject to all applicable federal and state privacy protections through the term of this Agreement.

4. SOPPA Compliance, 105 ILCS 85/15(4)

(a) The information ("Data") transmitted to Embrace® for storage may include, but is not limited to, student identification; attendance; educational and therapeutic recommendations; educational and therapeutic completion; communications between administration, educators, staff and parents/guardians regarding student, their education and any necessary assistance students may require.

(b) The services provided by Embrace® are set forth below.

(c) The Party's expressly agree and state that in performing its obligations hereunder Embrace® is acting as a "school official" with a legitimate educational interest in the School District data and it is performing an institutional service or function under this Agreement for which the District would otherwise use its own employees. Embrace's® use of the data is under the direct control of the District and such data shall only be used for authorized purposes. Embrace® shall not re-disclose such information to third parties or affiliates (unless permitted or required under law) without permission from the District or pursuant to a court order.

(d) Data Breach.

a. In the event of a data breach attributed to Embrace®, which means an unauthorized disclosure, access, alteration, or use of School District data by Embrace® or its employees, Embrace® shall promptly institute the following: (1) notify the School District by telephone and email as soon as practicable, but no later than twenty-four hours after Embrace® becomes aware of the data breach; (2) provide the School District with the name and contact information for an Embrace® employee who shall serve as the Embrace's® primary security contact; (3) assist the School District with any investigation, including interviews of Embrace® employees and review of all relevant records; (4) assist the School District with notification(s) the School District deems reasonably necessary related to the security breach; (5) provision of credit monitoring for one year to those students whose covered information was exposed in a manner during the breach such that a reasonable person would believe it could impact their credit or financial security; and (6) pay the reasonable legal fees (or assume the defense of the district at Embrace's discretion), reasonable audit costs, fines, and any other fees or damages imposed against the school solely as a result of Embrace's actions or failure to act.

b. In the event of a data breach attributed to the School District, which means an unauthorized disclosure, access, alteration, or use of School District data the School District shall promptly: (1) notify Embrace® by telephone and email as soon as practicable, but no later than twenty-four hours after the School District becomes aware of the data breach; (2) provide Embrace® with the name and contact information for an employee of the School who shall serve as the School District's primary security contact; (3) assist Embrace® with any investigation, including interviews with School employees and review of all relevant records. Embrace® shall have no liability for any damages related to a data breach due to or caused by School District's software, equipment, personnel, students or unauthorized third-parties using or exceeding their authorized use of the School's access, computer system or network.(4) pay the reasonable legal fees (or assume the defense of Embrace at the district's discretion), reasonable audit costs, and any other fines, fees or damages imposed against Embrace solely as a result of district's actions or failure to act.

(e) Embrace® shall provide all notifications required by the State Board of Education or any other State or federal law. Embrace® shall not provide any other notices without prior written permission from the School District.

(f) Upon written notification by District that student information is no longer needed for the purposes of this Agreement, Embrace® shall delete the information within 60 days so long as Embrace® is not required by law or court order to retain the same. Embrace® is not responsible for the deletion of any data due to District request.

(g) This Agreement and any amendments hereto must be published on the School District's website or, if the District does not have a website, made available for public review at its administrative office.

5. RESTRICTIONS. You may not copy, modify, adapt or translate any Embrace® software. You may not reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code of any Embrace® software.

You may not rent, lease, sell, sublicense, assign or transfer your rights in the website, or authorize any portion of the website and its related software to be copied onto another individual or legal entity's computer except as may be permitted herein.

You may not allow access or use of our website or software for any other purpose than agreed to in advance between Embrace® and you.

6. LIMITED WARRANTY. Embrace® warrants to the licensee that the website will permit the licensee to produce, fill-out, and print the 504 forms for the period of time outlined in the current contract. All warranty claims must be made within the current contract period. If the website or software does not perform as above, the entire liability of Embrace® and your sole and exclusive remedy will be limited to a prorated refund of the license fee you have paid Embrace®. This limited warranty is the only warranty provided by Embrace®. Embrace® expressly disclaims all other warranties, either expressed or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose with regard to the website, software and accompanying written materials.

7. DISCLAIMER. Your use of the website is at your sole risk. The website, including the information, services and content is provided on an "as is", "as available", and "with all faults" basis. Embrace® makes no representations, warranties, conditions, or guarantees as to the usefulness, quality, suitability, truth, accuracy, or completeness of the website and/or the forms produced therefrom.

Embrace® does not warrant to the licensee that the forms that may be produced from the website will comply with federal or state laws or regulations, including those which limit the extent to which the information may be disclosed to third parties.

Embrace® will take all commercially reasonable steps to provide an uninterrupted, timely, secure, and error-free website. Nonetheless, Embrace® makes no warranty or representation that (a) the website will be uninterrupted, timely, secure, or error-free; or (b) the results that may be obtained from the use of the website will be accurate or reliable.

You assume all risk for any damage to your computer, computer systems, network or loss of data that results from using the website or software, including any damages resulting from computer viruses.

8. DISTRICT E-SIGNATURE USAGE. Embrace® has the ability to include electronic signatures. If your District is using electronic signatures in the Embrace® system it agrees to hold Embrace® harmless against any and all claims that may arise out of the use of this feature. If you choose not to use electronic signatures for either your staff or all meeting attendees, you must notify your implementation specialist and verify that they are not available in your system.

All Parties shall ensure that the person entering an e-signature onto any Embrace® document is an authorized signatory. The e-signature of any Party or Person is to be considered as an original signature, and the document transmitted is to be considered to have the same binding effect as an original signature on an original document. All e-signatures shall be subject to the Uniform Electronic Transactions Act and/or any similar State statutes which have jurisdiction over the transactions of the Parties; this applies to any Parties or end-user's use of Embrace® software's electronic signature functionality. District, and any person using electronic signature functionality, agrees to hold Embrace® harmless for any and all claims which may arise out of their use of that feature. Documents which contain e-signatures may be preserved by Embrace® longer than the duration of the Agreement for the purposes of enforcement of rights and obligations.

Any form or document (including this Agreement) signed electronically between the Parties is to be treated as an original document. All Parties hereto shall ensure that the person entering an e-signature onto any Embrace® document is an authorized signatory. The e-signature of any Party or Person is to be considered as an original signature, and the document transmitted is to be considered to have the same binding effect as an original signature on an original document.

9. LIMITATION OF LIABILITY. In no event will Embrace® be liable to you for any loss, damages, claims, or costs whatsoever including any consequential, indirect or incidental damages, any lost profits or lost savings, any damages resulting from business interruption, personal injury or failure to meet any duty of care, or claims by a third party.

10. SERVICES PROVIDED: Embrace® agrees to provide the following services:

- Restrictive access to the website to allow for multiple levels of users, providing each level with only the access that they need
- Servers, security, and hosting to ensure that our programs are secure, fast, and available
- Multiple support channels available to all users
- A user management system will be included allowing a system administrator to create new users, edit existing users, and delete users
- Secure socket layer ("SSL") and session tracking for user authorization (the SSL is the component of the software which encrypts the information going between the website and the user, and confirms the identity of the host and the user)
- Website hosting
- Maintenance and updates
- Daily backups
- 99.99% uptime guarantee

11. 504 YEARLY COSTS. The initial contract is for a six month period from January 1, 2022 to June 30, 2022. (Prices apply to individual districts, cooperatives, joint agreements, and associations.) Custom forms and/or programs, if requested, are an additional cost and will be billed on an individual basis.

Program Subscription	Price	QTY	Subtotal
Embrace504® Annual Subscription Annual Subscription Fee	$1,050.00	1	$1,050.00
Less Prorated Months (July 2021 - December 2021)	-$525.00	1	-$525.00
			$525.00

Implementation Services and Training (Initial Year Only)			
Non-Recurring Implementation Services	$750.00	1	$750.00
Training: (2) Webinar Sessions	$250.00	1	$250.00
			$1,000.00

Subtotal	**$1,525.00**
Total Cost for 21-22 School Year	**$1,525.00**

* Pricing good for 90 days from the date delivered to prospective client.

All quoted prices apply to individual districts, cooperatives, joint agreements, and associations. Custom forms, software and/or programs are available from Embrace® and, if requested, will be subject to a separate Agreement between you and us. Customized work is an additional cost and will be billed separately.

12. GENERAL PROVISIONS. If any part of this Agreement is found void and unenforceable, it will not affect the validity of the balance of this Agreement, which will remain valid and enforceable according to its terms.

13. INDEMNITY. You agree to hold us harmless from any and all liabilities, losses, actions, damages, or claims (including all reasonable expenses, costs, and attorney fees) arising out of or relating to any use of, or reliance on the website and its related software.

14. DURATION. This contract for website access to Embrace504® is initially for a six month period.

15. AUTOMATIC CONTRACT RENEWAL. Unless cancelled by a Party hereto this Agreement and any accessory components selected by the district will automatically renew, on its last effective date, for successive one-year terms. The terms of this Master Contract, along with any pricing adjustments provided by Embrace to District at least one hundred and twenty (120) days prior to the annual renewal date shall apply.

16. NON-RENEWAL OF CONTRACT. In the event that you do not enter into a Renewal Contract, Embrace® will maintain your database information in read-only format for one (1) year from the date of termination of this Contract or subsequent failure to renew. Embrace® is not responsible for the loss of any information after termination or failure to renew the Agreement on your behalf.

17. ENTIRE AGREEMENT. This Agreement constitutes the entire Agreement and understanding between the parties in relation to the subject matter hereof and there are no premises, representations, conditions, provisions, or terms related thereto other than those set forth in this Agreement.

18. GOVERNING LAW. This Agreement will be governed by and construed in accordance with the laws of the State of Illinois.

19. **ARBITRATION**. Any and all disputes between us and you shall be resolved through mandatory Arbitration under the American Arbitration Association Rules. All arbitrations shall be held in Highland, IL.

20. **VENUE.** We and you (through your signature on this Agreement) agree that the only venue(s) holding jurisdiction for any suit between the parties to compel or enforce arbitration of this Agreement or any Renewal thereof is the third Judicial Circuit, Madison County, Illinois or the United States District Court for the Southern District of Illinois.

21. **CAPTIONS**. The captions for the paragraphs of this Agreement shall not be deemed to have legal significance, and are simply designed as an aid in reading and to represent the general terms of the paragraph involved.

22. **BENEFIT**. This Agreement shall be binding upon and inure to the benefit of the parties, their successors, assigns, beneficiaries, heirs, executors, administrators, and legal representatives.

Licensor:	**Brecht's Database Solutions, Inc. d/b/a EMBRACE®**
FEIN: 20-4100129	August R. Brecht, President
	Ernest Olson by Braun
Licensee:	The Board of Trustees of Illinois State University
FEIN: 37-6014070	Ernest Olson, Director of Purchases

KLF / J. Smith

Certifications and Additional Terms

Vendor acknowledges and agrees that compliance with this subsection in its entirety for the term of any resulting contract and any renewals is a material requirement and condition of the contract. By executing the contract Vendor certifies compliance with this subsection in its entirety, and is under a continuing obligation to remain in compliance and report any non-compliance.

This subsection, in its entirety, also applies to subcontractors used on this contract. Vendor shall include these Standard Certifications in any subcontract used in the performance of the contract using the Standard Subcontractor Certification form provided by the State.

If the contract extends over multiple fiscal years, including the initial term and all renewals, Vendor and its subcontractors shall confirm compliance with this section in the manner and format determined by the State by the date specified by the State and in no event later than July 1 of each year that the contract remains in effect.

If the Parties determine that any certification in this section is not applicable to the contract it may be stricken without affecting the remaining subsections.

1. As part of each certification, Vendor acknowledges and agrees that should Vendor or its subcontractors provide false information, or fail to be or remain in compliance with the Standard Certification requirements, one or more of the following sanctions will apply:

    - the contract may be void by operation of law,
    - the State may void the contract, and
    - the Vendor and its subcontractors may be subject to one or more of the following: suspension, debarment, denial of payment, civil fine, or criminal penalty.

    Identifying a sanction or failing to identify a sanction in relation to any of the specific certifications does not waive imposition of other sanctions or preclude application of sanctions not specifically identified.

2. Vendor certifies it and its employees will comply with applicable provisions of the United States Civil Rights Act, Section 504 of the Federal Rehabilitation Act, the Americans with Disabilities Act, and applicable rules in performance of this contract.

3. **This applies to individuals, sole proprietorships, partnerships and LLCs, but is otherwise not applicable**. Vendor, if an individual, sole proprietor, partner or an individual as member of a LLC, certifies he/she is not in default on an educational loan. 5 ILCS 385/3

4. Vendor certifies that is has reviewed and will comply with the Department of Employment Security Law (20 ILCS 1005/1005-47) as applicable.

5. **This applies only to certain service contracts and does NOT include contracts for professional or artistic services.** To the extent there was a current Vendor providing the services covered by this contract and the employees of that Vendor who provided those services are covered by a collective bargaining agreement, Vendor certifies (i) that it will offer to assume the collective bargaining obligations of the prior employer, including any existing collective bargaining agreement with the bargaining representative of any existing collective bargaining unit or units performing substantially similar work to the services covered by the contract subject to its bid or offer; and (ii) that it shall offer employment to all employees currently employed in any existing bargaining unit who perform substantially similar work to the work that will be performed pursuant to this contract. This does not apply to heating, air conditioning, plumbing and electrical service contracts. 30 ILCS 500/25-80

6. Vendor certifies it has neither been convicted of bribing or attempting to bribe an officer or employee of the State of Illinois or any other State, nor made an admission of guilt of such conduct that is a matter of record. 30 ILCS 500/50-5

7. If Vendor has been convicted of a felony, Vendor certifies at least five years have passed after the date of completion of the sentence for such felony, unless no person held responsible by a prosecutor's office for the facts upon which the conviction was based continues to have any involvement with the business. 30 ILCS 500/50-10

8. If Vendor or any officer, director, partner, or other managerial agent of Vendor has been convicted of a felony under the Sarbanes-Oxley Act of 2002, or a Class 3 or Class 2 felony under the Illinois Securities Law of 1953, Vendor certifies at least five years have passed since the date of the conviction. Vendor further certifies that it is not barred from being awarded a contract. 30 ILCS 500/50-10.5

9. Vendor certifies it is not barred from having a contract with the State based upon violating the prohibitions related to either submitting/writing specifications or providing assistance to an employee of the State of Illinois by reviewing, drafting, directing, or preparing any invitation for bids, a request for proposal, or request of information, or similar assistance (except as part of a public request for such information). 30 ILCS 500/50-10.5(e)

10. Vendor certifies that it and its affiliates are not delinquent in the payment of any debt to the State (or if delinquent have entered into a deferred payment plan to pay the debt. 30 ILCS 500/50-11, 50-60

11. Vendor certifies that it and all affiliates shall collect and remit Illinois Use Tax on all sales of tangible personal property into the State of Illinois in accordance with provisions of the Illinois Use Tax Act. 30 ILCS 500/50-12

12. Vendor certifies that it has not been found by a court or the Pollution Control Board to have committed a willful or knowing violation of the Environmental Protection Act within the last five years, and is therefore not barred from being awarded a contract. 30 ILCS 500/50-14

13. Vendor certifies it has neither paid any money or valuable thing to induce any person to refrain from bidding on a State contract, nor accepted any money or other valuable thing, or acted upon the promise of same, for not bidding on a State contract. 30 ILCS 500/50-25

14. Vendor certifies it has read, understands and is not knowingly in violation of the “Revolving Door” provisions of the Illinois Procurement Code. 30 ILCS 500/50-30

15. Vendor certifies that if it hires a person required to register under the Lobbyist Registration Act to assist in obtaining any State contract, that none of the lobbyist’s costs, fees, compensation, reimbursements or other remuneration will be billed to the State. 30 ILCS 500/50-38

16. Vendor certifies that it will not retain a person or entity to attempt to influence the outcome of a procurement decision for compensation contingent in whole or in part upon the decision or procurement. 30 ILCS 500/50-38

17. Vendor certifies it will report to the Illinois Attorney General and the Chief Procurement Officer any suspected collusion or other anti-competitive practice among any bidders, offerors, contractors, proposers, or employees of the State. 30 ILCS 500/50-40, 50-45, 50-50

18. Vendor certifies that if it is awarded a contract through the use of the preference required by the Procurement of Domestic Products Act, then it shall provide products pursuant to the contract or subcontract that are manufactured in the United States. 30 ILCS 517

19. Vendor certifies steel products used or supplied in the performance of a contract for public works shall be manufactured or produced in the United States, unless the executive head of the procuring Agency/University grants an exception. 30 ILCS 565

20. Drug Free Workplace

20.1 If Vendor employs 25 or more employees and this contract is worth more than $5,000, Vendor certifies it will provide a drug free workplace pursuant to the Drug Free Workplace Act

20.2 If Vendor is an individual and this contract is worth more than $5000, Vendor certifies it shall not engage in the unlawful manufacture, distribution, dispensation, possession, or use of a controlled substance during the performance of the contract. 30 ILCS 580

21. Vendor certifies that neither Vendor nor any substantially owned affiliate is participating or shall participate in an international boycott in violation of the U.S. Export Administration Act of 1979 or the applicable regulations of the United States Department of Commerce. 30 ILCS 582

22. Vendor certifies that no foreign-made equipment, materials, or supplies furnished to the State under the contract have been or will be produced in whole or in part by forced labor or indentured labor under penal sanction. 30 ILCS 583

23. Vendor certifies that no foreign-made equipment, materials, or supplies furnished to the State under the contract have been produced in whole or in part by the labor of any child under the age of 12. 30 ILCS 584

24. This applies to information technology contracts and is otherwise not applicable. Vendor certifies that information technology, including electronic information, software, systems and equipment, developed or provided under this contract comply with the applicable requirements of the Illinois Information Technology Accessibility Act Standards as published at (www.dhs.state.il.us/iitaa). 30 ILCS 587

25. **This only applies to vendors who own residential buildings but is otherwise not applicable.** Vendor certifies, if it owns residential buildings, that any violation of the Lead Poisoning Prevention Act has been mitigated. 410 ILCS 45

26. Vendor certifies it has not been convicted of the offense of bid rigging or bid rotating or any similar offense of any state or of the United States. 720 ILCS 5/33 E-3, E-4

27. Vendor certifies it complies with the Illinois Department of Human Rights Act and rules applicable to public contracts, which include providing equal employment opportunity, refraining from unlawful discrimination, and having written sexual harassment policies. 775 ILCS 5/2-105

28. Vendor certifies it does not pay dues to or reimburse or subsidize payments by its employees for any dues or fees to any "discriminatory club." 775 ILCS 25/2

29. Vendor warrants and certifies that it and, to the best of its knowledge, its subcontractors have and will comply with Executive Order No. 1 (2007). The Order generally prohibits Vendors and subcontractors from hiring the then-serving Governor's family members to lobby procurement activities of the State, or any other unit of government in Illinois including local governments if that procurement may result in a contract valued at over $25,000. This prohibition also applies to hiring for that same purpose any former State employee who had procurement authority at any time during the one-year period preceding the procurement lobbying activity.

30. Vendor certifies that if an individual, sole proprietor, partner or an individual as a member of a LLC, he/she has not received an early retirement incentive prior to 1993 under Section 14-108.3 or 16-133.3 of the Illinois Pension Code or an early retirement incentive on or after 2002 under Section 14-108.3 or 16-133.3 of the Illinois Pension Code. 30 ILCS 105/15a; 40 ILCS 5/14-108.3; 40 ILCS 5/16-133

31. Vendor certifies that it has read, understands, and is in compliance with the registration requirements of the Elections Code (10 ILCS 5/9-35) and the restrictions on making political contributions and related requirements of the Illinois Procurement Code. Vendor will not make a political contribution that will violate these requirements. 30 ILCS 500/20-160 and 50-37.

32. A person (other than an individual acting as a sole proprietor) must be a duly constituted legal entity and authorized to transact business or conduct affairs in Illinois prior to submitting a bid or offer. If you do not meet these criteria, then your bid or offer will be disqualified. 30 ILCS 500/20-43

Brecht's Database Solutions, Inc. d/b/a EMBRACE

August Brecht President

The Board of Trustees of Illinois State University

Ernest Olson by Brom

Ernest Olson, Director of Purchases

Additional Terms:

~~**Assignment and Subcontracting**: (30 ILCS 500/20-120)   Any contract may not be assigned or transferred in whole or in part by Vendor without the prior written consent of the University. For purposes of this section, subcontractors are those specifically hired by the Vendor to perform all or part of the work covered by the contract. Vendor shall describe the names and addresses of all subcontractors to be utilized by Vendor in the performance of the resulting contract, together with a description of the work to be performed by the subcontractor and the anticipated amount of money that each subcontractor is expected to receive pursuant to a subsequent contract. Vendor shall notify the University in writing of any additional or substitute subcontractors hired during the term of a resulting contract, and shall supply the names and addresses and the expected amount of money that each new or replaced subcontractor will receive pursuant to the Contract. All subcontracts must include the same certifications and disclosures that Vendor must make as a condition of their contract.~~

~~**Audit / Retention of Records**: (30 ILCS 500/20-65)   Vendor and its subcontractors shall maintain books and records relating to the performance of the resulting contract or subcontract and necessary to support amounts charged to the University. Books and records, including information stored electronically, shall be maintained by the Vendor for a period of three years from the later of the date of final payment under the contract or completion of the contract, and by the subcontractor for a period of three years from the later of final payment under the term or completion of the subcontract. If federal funds are used to pay contract costs, the Vendor and its subcontractors must retain its records for a minimum of five years after completion of work. Books and records required to be maintained under this section shall be available for review or audit by representatives of: the University, the Auditor General, the Executive Inspector General, the Chief Procurement Officer, State of Illinois internal auditors or other governmental entities with monitoring authority, upon reasonable notice and during normal business hours. Vendor and its subcontractors shall cooperate fully with any such audit and with any investigation conducted by any of these entities. Failure to maintain books and records required by this section shall establish a presumption in favor of the University for the recovery of any funds paid by the University under the contract for which adequate books and records are not available to support the purported disbursement. The Vendor or subcontractors shall not impose a charge for audit or examination of the Vendor's books and records.~~

Availability of Appropriation (30 ILCS 500/20-60): Any resulting contract is contingent upon and subject to the availability of funds. The University, at its sole option, may terminate or suspend this contract, in whole or in part, without penalty or further payment being required, if the Illinois General Assembly or the federal funding source fails to make an appropriation sufficient to pay such obligation. If funds needed are insufficient for any reason, the University has discretion on which contracts will be funded.

Transportation Sustainability Procurement Program Act (30 ILCS 530/10 (b): All contracts for freight, small package delivery, and any transportation of cargo require providers to report the amount of energy the service provider consumed to provide those services to the State and the amount of associated greenhouse gas emissions, including energy use and greenhouse gases emitted as a result of the provider's use of electricity in its facilities and the energy use and greenhouse gas emissions by the service provider's subcontractors in the performance of those services.

Expatriated Entity: For purposes of this provision, an expatriated entity is an entity that meets the definition outlined in 30 ILCS 500/1-15.120. Per 30 ILCS 500/50-17, no business or member of a unitary business group, as defined in the Illinois Income Tax Act, shall enter into a contract with a State agency under this Code if that business or any member of the unitary business group is an expatriated entity unless the Chief Procurement Officer:

a) Has determined the contract is awarded as a sole source; or
b) the purchase is of pharmaceutical products, drugs, biologics, vaccines, medical supplies, or devices used to provide medical and health care or treat disease or used in medical or research diagnostic tests, and medical nutritionals regulated by the Food and Drug Administration under the Federal Food, Drug, and Cosmetic Act.

Sexual Harassment Policy: Per 30 ILCS 500/50-80, Vendor agrees that it has a sexual harassment policy that meets the requirements of or is otherwise in accordance with Section 2-105 of the Illinois Human Rights Act (775 ILCS 5/2-105). Vendor agrees to provide a copy of the policy to the University upon request.

Standard Student Data Privacy Agreement
IL-NDPA v1.0a

School District or LEA
The Board of Trustees of Illinois State University Laboratory Schools

and

Provider
Brecht's Database Solutions, Inc. DBA: Embrace®

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:

The Board of Trustees of Illinois State University Laboratory Schools, located at 100 North University Street, Normal, IL 61790 (the "**Local Education Agency**" or "**LEA**")
and
Brecht's Database Solutions, Inc. DBA: Embrace®, located at 1000 Broadway, Suite 300, Highland, IL 62249 (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, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H". (Optional)**

□ 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 LEA for this DPA is:

Title: Director of Purchases

Name: Ernest Olson
Address: 100 North University Street, Normal, IL 61790
Email: ISUPurchasing@ilstu.edu
Phone: (306) 438-1946

The designated representative for the Provider for this DPA is:

Name: August R. Brecht
Title: President
Address: P.O. Box 305, Highland, IL 62249
Phone: (888) 437-9326
Email: gus@embraceeducation.com

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

LEA: The Board of Trustees of Illinois State University Laboratory Schools

By: Ernest Olson by

Date: 12·16·21

Printed Name: Ernest Olson

Title/Position: Director of Purchases

Provider: Brecht's Database Solutions, Inc. D/B/A Embrace®

By:

Date: 1/21/22

Printed Name: August R. Brecht

Title/Position: President

STANDARD CLAUSES

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 herto 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 servicesor 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 to **Exhibit "H"**. 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 **<u>Exhibit “E”</u>**), 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. <u>Termination</u>. 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. <u>Effect of Termination Survival</u>. If the Service Agreement is terminated, the Provider shall destroy all of LEA’s Student Data pursuant to Article IV, section 6.

3. <u>Priority of Agreements</u>. 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 **Exhibit "H"**, the SDPC Standard Clauses, and/or the Supplemental State Terms, **Exhibit "H"** will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. <u>Entire Agreement</u>. 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. <u>Severability</u>. 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. <u>Governing Law; Venue and Jurisdiction</u>. 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 herby.

7. <u>Successors Bound</u>: 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

EmbraceIEP® is web-based administrative software designed to allow school staff to document all aspects of the IEP process from evaluations to accommodations, services and goals. Our streamlined, easy to use software, allows districts to easily document all data necessary for complying with state and federal rules and regulations. Districts can customize forms to meet their unique needs.

Embrace504® is web-based administrative software designed to allow school staff to document all aspects of the 504 process from evaluations to accommodations, services and goals. Our streamlined, easy to use software, allows districts to easily document all data necessary for complying with state and federal rules and regulations. Districts can customize forms to meet their unique needs.

EmbraceMTSS® is web-based administrative software designed software to streamline MTSS documentation and provides staff with the most efficient means to document and monitor student plans.

EmbraceDS® is web-based administrative software designed to assist districts in documenting services delivered to students and to claim Medicaid reimbursement for services delivered to Medicaid eligible students.

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.	X
Application Technology Meta Data	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	X
Assessment	Observation data	X
Assessment	Other assessment data-Please specify:	X
Attendance	Student school (daily) attendance data	X
Attendance	Student class attendance data	X
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	X
Demographics	Date of Birth	X
Demographics	Place of Birth	X
Demographics	Gender	X
Demographics	Ethnicity or race	X
Demographics	Language information (native, or primary language spoken by student)	X
Demographics	Other demographic information-Please specify:	X
Enrollment	Student school enrollment	X
Enrollment	Student grade level	X
Enrollment	Homeroom	X

Category of Data	Elements	Check if Used by Your System
Enrollment	Guidance counselor	X
Enrollment	Specific curriculum programs	
Enrollment	Year of graduation	X
Enrollment	Other enrollment information-Please specify:	X
Parent/Guardian Contact Information	Address	X
Parent/Guardian Contact Information	Email	X

Category of Data	Elements	Check if Used by Your System
Parent/Guardian Contact Innformation	Phone	X
Parent/Guardian ID	Parent ID number (created to link parents to students)	X
Parent/Guardian Name	First and/or Last	X
Schedule	Student scheduled courses	X
Schedule	Teacher names	X
Special Indicator	English language learner information	X
Special Indicator	Low income status	X
Special Indicator	Medical alerts/ health data	X
Special Indicator	Student disability information	X
Special Indicator	Specialized education services (IEP or 504)	X
Special Indicator	Living situations (homeless/foster care)	X
Special Indicator	Other indicator information-Please specify:	X
Student Contact Information	Address	X
Student Contact Information	Email	X
Student Contact Information	Phone	X
Student Identifiers	Local (School district) ID number	X
Student Identifiers	State ID number	X
Student Identifiers	Provider/App assigned student ID number	X
Student Identifiers	Student app username	
Student Identifiers	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)	

Category of Data	Elements	Check if Used by Your System
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	X
Student work	Other student work data – Please specify:	X
Transcript	Student course grades	
Transcript	Student course data	

Category of Data	Elements	Check if Used by Your System
Transcript	Student course grades/ performance scores	
Transcript	Other transcript data - Please specify	
Transportation	Student bus assignment	
Transportation	Student pick up and/or drop off location	X
Transportation	Student bus card ID number	
Transportation	Other transportation data — Please specify:	X
Other	Please list each additional data element used, stored, or collected by your application: Embrace® is a system where school districts collect and document information for the purpose of writing IEPs, 504 plans, tracking MTSS data and recording the delivery of services. School districts, based on state and federal regulations, determine what data they will enter into the Embrace® system.	X
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 allpersonally 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 reasonableavailable 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 CFR § 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

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: All SOPPA covered information by definition in SOPPA.

□ 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: labschools@ilstu.edu should be contacted to determine the appropriate method of transfer. Following disposition of data, the provider is still required to destroy data.

3. Schedule of Disposition

Data shall be disposed of by the following date:

☒ As soon as commercially practicable.

□ By

4. Signature

_________________________ _________________________

Authorized Representative of LEA Date

5. Verification of Disposition of Data

_________________________ _________________________

Authorized Representative of Company Date

EXHIBIT “E”
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Illinois State University Laboratory Schools(“Originating LEA”) which is dated 6/18/21, to any other LEA (“Subscribing LEA”) who accepts this General Offer of Privacy Terms (“General Offer”) through its signature below. This General Offer shall extend only to privacy protections, and Provider’s signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider’s signature to this Form. Subscribing LEAs should send the signed **Exhibit "E”** to Provider at the following email address: success@embraceeducation.com.

PROVIDER: Brecht's Database Solutions, Inc. DBA: Embrace®

BY:_______________________________ Date: ______________________

Printed Name: August R. Brecht Title/Position: President

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the LEA and Brecht's Database Solutions, Inc. DBA: Embrace®

**PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

Subscribing LEA:

BY: _________________________________ Date:________________________

Printed Name: ___________________________ Title/Position: ___________________________

SCHOOL DISTRICT NAME:____

DESIGNATED REPRESENTATIVE OF LEA:

Name: ____

Title: ______________________________

Address: ______________________________

Telephone Number: ______________________________

Email: ______________________________

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider .

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
X	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)

Please visit http://www.edspex.org for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

<u>EXHIBIT "G"</u>
Supplemental SDPC (Student Data Privacy Consortium)
State Terms for Illinois
Version IL-NDPAv1.0a (Revised March 15, 2021)

This **<u>Exhibit G</u>**, Supplemental SDPC State Terms for Illinois ("Supplemental State Terms"), effective simultaneously with the attached Student Data Privacy Agreement ("DPA") by and between The Board of Trustees of Illinois State University Laboratory Schools(the "Local Education Agency" or "LEA") and Brecht's Database Solutions, Inc DBA: Embrace® (the
"Provider"), is incorporated in the attached DPA and amends the DPA (and all supplemental terms and conditions and policies applicable to the DPA) as follows:

1. <u>Compliance with Illinois Privacy Laws</u>. In performing its obligations under the Agreement, the Provider shall comply with all Illinois laws and regulations pertaining to student data privacy, confidentiality, and maintenance, including but not limited to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/, and Local Records Act (“LRA”), 50 ILCS 205/.

2. <u>Definition of "Student Data."</u> In addition to the definition set forth in **Exhibit "C"**, Student Data includes any and all information concerning a student by which a student may be individually identified under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school student records" as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)) (c) “records” as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) “personal information” as defined in Section 530/5 of PIPA.

3. <u>School Official Designation</u>. Pursuant to Article I, Paragraph 1 of the DPA Standard Clauses, and in accordance with FERPA, ISSRA and SOPPA, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; is under the direct control of the LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose and in furtherance of such legitimate educational interest.

4. <u>Limitations on Re-Disclosure.</u> The Provider shall not re-disclose Student Data to any other party or affiliate without the express written permission of the LEA or pursuant to court order, unless such disclosure is otherwise permitted under SOPPA, ISSRA, FERPA, and MHDDCA. Provider will not sell or rent Student Data. In the event another party, including law enforcement or a government entity, contacts the Provider with a request or subpoena for Student Data in the possession of the Provider, the Provider shall redirect the other party to seek the data directly from the LEA. In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure.

5. <u>Notices.</u> Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or four (4) days after mailing, if by first-class mail, postage prepaid.

6. <u>Parent Right to Access and Challenge Student Data.</u> The LEA shall establish reasonable procedures pursuant to which a parent, as that term is defined in 105 ILCS 10/2(g), may inspect and/or copy Student Data and/or challenge the accuracy, relevance or propriety of Student Data, pursuant to Sections 5 and 7 of ISSRA (105 ILCS 10/5; 105 ILCS 10/7) and Section 33 of SOPPA (105 ILCS 85/33). The Provider shall respond to any request by the LEA for Student Data in the possession of the Provider when Provider cooperation is required to afford a parent an opportunity to inspect and/or copy the Student Data, no later than 5 business days from the date of the request. In the event that a parent contacts the Provider directly to inspect and/or copy Student Data, the Provider shall refer the parent to the LEA, which shall follow the necessary and proper procedures regarding the requested Student Data.

7. Corrections to Factual Inaccuracies. In the event that the LEA determines that the Provider is maintaining Student Data that contains a factual inaccuracy, and Provider cooperation is required in order to make a correction, the LEA shall notify the Provider of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, the Provider shall correct the factual inaccuracy and shall provide written confirmation of the correction to the LEA.

8. Security Standards. The Provider shall implement and maintain commercially reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect Student Data from unauthorized access, destruction, use, modification, or disclosure, including but not limited to the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the Student Data (a "Security Breach"). For purposes of the DPA and this **Exhibit "G"**, "Security Breach" does not include the good faith acquisition of Student Data by an employee or agent of the Provider or LEA for a legitimate educational or administrative purpose of the Provider or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure.

9. Security Breach Notification. In addition to the information enumerated in Article V, Section 4(1) of the DPA Standard Clauses, any Security Breach notification provided by the Provider to the LEA shall include:

a. A list of the students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known;

and

b. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.

10. Reimbursement of Expenses Associated with Security Breach. In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, without regard to any limitation of liability provision otherwise agreed to between Provider and LEA, including but not limited to costs and expenses associated with:

a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;

b. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the student's credit or financial security;

c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA as a result of the security breach;

and

d. Providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws.

11. Transfer or Deletion of Student Data. The Provider shall review, on an annual basis, whether the Student Data it has received pursuant to the DPA continues to be needed for the purpose(s) of the Service Agreement and this DPA. If any of the Student Data is no longer needed for purposes of the Service Agreement and this DPA, the Provider will provide written notice to the LEA as to what Student Data is no longer needed. The Provider will delete or transfer Student Data in readable form to the LEA, as directed by the LEA (which may be effectuated through Exhibit D of the DPA), within 30 calendar days if the LEA requests deletion or transfer of the Student Data and shall provide written confirmation to the LEA of such deletion or transfer. Upon termination of the Service Agreement between the Provider and LEA, Provider shall conduct a final review of Student Data within 60 calendar days.

If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving the request.

Any provision of Student Data to the LEA from the Provider shall be transmitted in a format readable by the LEA.

12. Public Posting of DPA. Pursuant to SOPPA, the LEA shall publish on its website a copy of the DPA between the Provider and the LEA, including this **Exhibit "G"**.

13. Subcontractors. By no later than (5) business days after the date of execution of the DPA, the Provider shall provide the LEA with a list of any subcontractors to whom Student Data may be disclosed or a link to a page on the Provider's website that clearly lists any and all subcontractors to whom Student Data may be disclosed. This list shall, at a minimum, be updated and provided to the LEA by the beginning of each fiscal year (July 1) and at the beginning of each calendar year (January 1).

14. DPA Term.

a. Original DPA. Paragraph 4 on page 2 of the DPA setting a three-year term for the DPA shall be deleted, and the following shall be inserted in lieu thereof: “This DPA shall be effective upon the date of signature by Provider and LEA, and shall remain in effect as between Provider and LEA 1) for so long as the Services are being provided to the LEA or 2) until the DPA is terminated pursuant to Section 15 of this **Exhibit "G"**, whichever comes first. The **Exhibit "E"** General Offer will expire three (3) years from the date the original DPA was signed.”

b. General Offer DPA. The following shall be inserted as a new second sentence in Paragraph 1 of Exhibit E: “The provisions of the original DPA offered by Provider and accepted by Subscribing LEA pursuant to this Exhibit E shall remain in effect as between Provider and Subscribing LEA 1) for so long as the Services are being provided to Subscribing LEA, or 2) until the DPA is terminated pursuant to Section 15 of this **Exhibit "G"**, whichever comes first.”

15. Termination. Paragraph 1 of Article VII shall be deleted, and the following shall be inserted in lieu thereof: “In the event either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service

Agreement has lapsed or been terminated. One party may terminate this DPA upon a material breach of this DPA by the other party. Upon termination of the DPA, the Service Agreement shall terminate."

16. Privacy Policy. The Provider must publicly disclose material information about its collection, use, and disclosure of Student Data, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.

17. Minimum Data Necessary Shared. The Provider attests that the Student Data request by the Provider from the LEA in order for the LEA to access the Provider's products and/or services is limited to the Student Data that is adequate, relevant, and limited to what is necessary in relation to the K-12 school purposes for which it is processed.

18. Student and Parent Access. Access by students or parents/guardians to the Provider's programs or services governed by the DPA or to any Student Data stored by Provider shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this DPA.

19. Data Storage. Provider shall store all Student Data shared under the DPA within the United States.

20. Exhibits "A" and "B". The Services described in **Exhibit "A"** and the Schedule of Data in **Exhibit "B"** to the DPA satisfy the requirements in SOPPA to include a statement of the product or service being provided to the school by the Provider and a listing of the categories or types of covered information to be provided to the Provider, respectively.

EXHIBIT "H"
Additional Terms or Modifications
Version___________

LEA and Provider agree to the following additional terms and modifications:

This is a free text field that the parties can use to add or modify terms in or to the DPA. If there are noadditional or modified terms, this field should read "None."

1. Article II, Section 5, has the following is added to the end of the section:

Embrace® is not responsible for any third parties to whom LEA transmits Student Data, or contracts for services, outside of those specifically provided by Embrace®.

2. Article V, Section 5, is deleted and replaced with the following:

In the event of a breach originating from LEA's use of the Service, LEA shall notify Embrace® 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. Both LEA and Embrace® shall assist each other with any reasonable investigation, including provision of relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation or as otherwise reasonably required by Embrace®. Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

3. Exhibit "D", Section 3, Schedule of Disposition includes and selects the following option:

Embrace® shall retain student data for one year in read-only format. All student data shall be deleted after expiration of that one-year. Embrace is not responsible for any lost student data after expiration of Contract.

4. Exhibit "G", Section 4, is deleted and replaced with:

Limitations on Re-Disclosure. The Provider shall not re-disclose Student Data to any Third Party or affiliate without the express written permission of the LEA or pursuant to court order, unless such disclosure is otherwise permitted under SOPPA,ISSRA,FERPA,and MHDDCA. In the event a Third Party, including law enforcement or a government entity, contacts the Provider with a request or subpoena for Student Data in the possession of the Provider, the Provider shall, if possible, redirect the Third Party to seek the data directly from the LEA. In the event the Provider is compelled to produce Student Data to a Third Party in compliance with a court order, if possible, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court orderrequiring such disclosure.

5. **Exhibit "G"**, Section 5, is deleted and replaced with:

Notices. Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or ten (10) days after mailing, if by first-class mail, postage prepaid.

6. Exhibit "G", Section 6, is deleted and replaced with:

Parent Right to Access and Challenge Student Data. The LEA shall establish reasonable procedures pursuant to which a parent, as that term is defined in 105 ILCS 10/2(g), may inspect and/or copy Student Data and/or challenge the accuracy, relevance or propriety of Student Data, pursuant to Sections 5 and 7 of ISSRA(105 ILCS 10/5; 105 ILCS 10/7) and Section 33 of SOPPA(105 ILCS 85/33). LEA shall have access to all Student Data in the possession of the Provider and shall be able to provide any parent an opportunity to inspect and/or copy the Student Data. Provider shall assist if necessary. In the event that a parent contacts the Provider directly to inspect and/or copy Student Data, the Provider shall refer the parent to the LEA, which shall follow the necessary and proper procedures regarding the requested Student Data.

7. Exhibit "G", Section 7, shall be deleted and replaced with:

Corrections to Factual Inaccuracies. In the event that the LEA determines that the Student Data contains a factual inaccuracy LEA shall correct the same no later than 90 calendar days after making such determination. Provider shall assist as necessary.

8. **Exhibit "G"**, Section 10, shall be deleted and replaced with:

Reimbursement of Expenses Associated with Security Breach.

a. In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all reasonable costs and expenses that the LEA incurs in investigating and remediating the Security Breach, including but not limited to costs and expenses associated with:

i. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;

ii. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the student's credit or financial security;

iii. Reasonable legal fees, audit costs, fines, and any other fees or damages imposed against the LEA as a result of the Security Breach; and

iv. Providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws.

b. In the event of a Security Breach that is solely attributable to the LEA and for which the LEA would not be immune from liability under the Illinois Local Governmental and Governmental Employees Tort Immunity Act (745 ILCS 10/1 et seq.) or other applicable immunities or defenses, the LEA shall reimburse the Company for any and all reasonable costs and expenses that the Company incurs in investigating and remediating the Security Breach, including but not limited to costs and expenses associated with reasonable legal fees, audit costs, and any other fees or damages sustained by the Company as a result of the Security Breach

KLF