
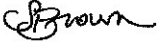


Firm or Company: Securly Dept LA 24957 Pasadena CA 91185-4957	<h1>Purchase Order</h1>  ILLINOIS STATE UNIVERSITY <i>Illinois' first public university</i>	P.O. Number: P0250472 P.O. Date: 03/03/25 Terms: Net 30 FOB Point: Destination Req Number: 0061068 Ship by: 03/05/25
Guidelines: 1. Show Purchase Order Number on all shipments and correspondence. 2. Do not include state, local or Federal Excise Taxes. ILLINOIS SALES TAX EXEMPTION ID NUMBER: E9991-3399 3. Inquiries, advice or changes must be sent to the Purchasing Department.	Invoice To: College of Education Campus Box 5300 PO# P0250472 Education@ilstu.edu Normal IL 61790-5300	Ship To: Illinois State University PO#: P0250472 Central Receiving 2016 Warehouse Road Normal, IL 61790-1520

Special Instructions

PER PROPOSAL DATED 3-31-2025 AND ATTACHED AGREEMENT.

Description	Part #	Quantity	Unit	Unit Price	Amount
Aware Premium subscription Term Period: 4/1/25 - 6/30/26		1,100		1.82	2,002.00
Filter Premium subscription Term Period: 4/1/25 - 6/30/26		1,100		4.87	5,357.00
Classroom Premium subscription Term Period: 4/1/25 - 6/30/26		1,000		3.82	3,820.00
Implementation Fee: Aware Standard		1		199.98	199.98
Implementation Fee: Classroom Standard		1		381.60	381.60

President Aondover Tarhule Signed By: 	For more information, contact Jesse Slater at jslate2@ilstu.edu, 309-438-2143	Total \$11,760.58
--	--	-------------------------------

Order Form

SECURLY	Dept LA 24957	Bill To Name	The Board of Trustees of Illinois State University
(Billing	Pasadena, CA 91185-4957	Bill To	(Illinois State University Laboratory Schools)
Address)	United States		, IL
Securly Contact	Sara Kohn	School Name	Illinois State University Laboratory Schools
	sara.kohn@securly.com	Contact Name	JORDAN Harrison
		Email	jjharr3@ilstu.edu
		Phone	3094384412

Invoice Information

Invoicing Contact Information:

Do you require Securly to reference a PO Number on your invoice (Y/N)?

Full Name:

If you selected YES, have you provided the purchase order? If yes, please put today's date. If not, please provide the date on which we should follow up with you in regards to receiving your PO:

Title:

PO Date:

Email:

Please note an invoice will not be sent until the PO has been received if YES is selected.

Phone:

Order Information

Payment Schedule	Upfront	Payment Terms	Net 30
Order Notes			Per the Illinois Prompt Payment Act
	Service Start Date: 04-01-2025		
	Paid Term Start Date: 07-01-2025		
	Service End Date: 06-30-2026		

Products & Services



Start Date	End Date	Quantity	Product	Product Type	Price	Subtotal
04-01-2025	06-30-2026	1,100	Aware Premium	Subscription	\$1.82	\$2,002.00
04-01-2025	06-30-2026	1,000	Classroom Premium	Subscription	\$3.82	\$3,820.00
04-01-2025	06-30-2026	1,100	Filter Premium	Subscription	\$4.87	\$5,357.00
		1	Implementation: Aware Standard	One Time	\$199.98	\$199.98
		1	Implementation: Classroom Standard	One Time	\$381.60	\$381.60
						\$11,760.58

Terms & Conditions

sb

Securly products and services are provided under the ~~Securly Terms and Conditions and Privacy Policy~~ attached **Terms of Service/Service Agreement including University Contract Addendum**. By signing this Order Form, customer agrees to these Terms and Conditions which constitute the entire agreement ("**Agreement**"), superseding any terms (including, but not limited to, any Customer's Purchase Order terms).

- Term of subscription license: Specified by "Term" beginning and end dates set forth above.
- Prices do not include sales tax, if applicable.
- The Federal Tax ID # for Securly is **46 078 9922**

Executed & Agreed:

CUSTOMER:

The Board of Trustees of Illinois State University

Signature

Name **Stacy Brown**

Title **Interim Director of Purchasing**

Date **3.6.25**

SECURLY:

Signature

Name **Emma Hayes**

Title **Deal Desk**

Date **3/27/25**

Terms of Service/Service Agreement

Effective Date: October 2024

This Agreement is made by and between Securly, Inc. and its affiliates and subsidiaries (“Company” or “Securly”), a Delaware corporation with offices at 5600 77 Center Drive, Suite 350 Charlotte, NC 28217, and its customer (“Customer”) listed on one or more order forms (each, an “Order”) executed by and between the parties (collectively, the “Agreement”).

Company will provide to Customer the cloud-based software products and services identified in the Order (collectively, the “Services” and, each, a “Service”). The Services may include, without limitation: Company’s cloud-based web filtering; online activity monitoring for cyberbullying; hall pass, visitor, and flex time management; auditing software; mobile device management software, tablet, and other computer assets; location tracking software, device control software for teacher classroom management, and any other software or services offered by Company, including all updates thereto and related documentation. Company shall provide all necessary user identifications and passwords for the Services for use by Customer’s employees, agents, independent contractors, students and parents/guardians, in each case as authorized by Customer to access the Services (“Users”).

In the event of a conflict between the terms of this Agreement and one or more written agreements signed by the parties setting forth the Customer’s requirements (collectively, the “Customer Terms”), the conflicting provision in the Customer Terms, **into which the attached University Laboratory School Software addendum is hereby incorporated**, shall take precedence.

1. Support

Company shall provide Customer with support services as specified in the Order (the "Support Services").

2. Ownership and Licenses

(a) Ownership of the Service; Intellectual Property. Company shall retain all title to and ownership of and all proprietary rights (including, but not limited to, all copyright, patent, trademark and trade secret rights) in and to the Services (including all software used to provide the Services and all portions thereof and all derivatives or improvements thereof and all related documentation), whether or not incorporated into or used with other software as a service, software or hardware. Customer's use of the Services does not constitute a sale of any of such software or any portion thereof. Company's name, logo, and the product names associated with the Services are trademarks of Company or third parties, and no right or license is granted herein to use them. Company hereby grants Customer, solely during the term of this Agreement, a limited, royalty-free, revocable license to use and install the Company provided software (which may include certificates and pack files) solely on Customer's machines and devices and only as necessary or appropriate to receive the Services (the "Client Software") and in accordance with the limitations (if any) set forth in the Order, and to use and reproduce a reasonable number of copies of any documentation solely to support Customer's use of the Services.

(b) Ownership of User Data. The Services may allow Customer to track and gather a range of data and information regarding its Users including, without limitation, information about students enrolled at Customer's educational institution, including the student's name, the student's (or student's family's) address, telephone number, email address, date of birth, place of birth, mother's maiden name, grades, social security number (or other governmental identification number), biometric information, and other information that alone or in combination would reasonably allow a person or entity to identify the student with reasonable certainty (collectively, "User Data"). Customer shall retain all title to and ownership of and all proprietary rights with respect to User Data, and shall be solely responsible for its use thereof. Customer is also responsible for securing and backing up its User Data and Company shall only restore lost User Data to its last-backup point if the loss was due to a fault in Company's Services or Support Services. Customer hereby grants Company a worldwide, royalty-free, and non-exclusive license to access and use User Data for the sole purpose of enabling Company to provide the Services, and for the limited purposes set forth in Company's Privacy Policy (described below). Customer also grants Company a worldwide, royalty-free, and non-exclusive license Customer's trademarks, service marks, and logos as required to provide the Services.

(c) Data Use. To the extent Company receives any personal information (as such term or any analogous term may be as defined under applicable law) from or on behalf of Customer in connection with Company's provision of Services to Customer under the Agreement ("Customer Personal Information"), Company will only use, retain, disclose and otherwise process such Customer Personal Information for the purpose of providing the Services or in order to comply with the law. Any such use, retention, disclosure, and processing will comply with all applicable state and federal laws, including, without limitation, the Family Education Rights and Privacy Act ("FERPA"). Company may disclose Customer Personal Information to its service providers as necessary for Company to provide the services to Customer, provided such disclosure shall be consistent with all applicable state and federal laws. Company will however not otherwise retain, use, or disclose Customer Personal Information for any purpose other than to perform the Services or outside of the direct business relationship between Customer and Company. Specifically, it will not sell, rent, release, disclose, disseminate, make available, transfer or otherwise communicate Customer Personal Information to any third party for monetary or other valuable consideration. Unless Customer has specified in writing a specific retention period for Customer Personal Information, Company will securely destroy such data when it is no longer needed to provide the services, in accordance with Company's standard data retention and destruction policies.

(d) Data sources. Customer acknowledges that, depending on the type of Services Company provides to Customer, Company may rely on publicly available or third-party data in order to provide the Services. Customer understands and agrees that Company has no responsibility for the accuracy, availability, reliability, or integrity of such data. Customer shall have the sole responsibility for the accuracy, quality, integrity, legality, reliability, and appropriateness of all User Data and shall maintain the minimum hardware, software, and connectivity configuration specified from time to time by Company as required for use of the Services (the "Supported Environment") (if any) described in the Order.

(e) Ownership of Reports and Analyses. Company may provide Customer with certain reports and analyses as part of the Services ("Reports"). Company shall retain all title to and ownership of and all proprietary rights with respect to such Reports, excluding Customer's Confidential Information as defined in Section 5 below. Company hereby grants Customer a non-exclusive, non-sublicensable, and non-transferable license, for the term of this Agreement, to use Reports strictly for Customer's own internal, legitimate, non-commercial, educational purposes.

(f) Mobile App and Parent/Guardian Usage. Customer acknowledges that Users may need to download the Company's mobile application from the relevant major mobile device provider app stores (Apple's App Store or Google Play) and that use of the Company's mobile application or website by parents/guardians is subject to Company's terms of service and Privacy Policy.

(g) Feedback. If Customer provides any ideas, suggestions or recommendations to Company regarding Company's software, products, services or technology ("Feedback"), such Feedback is provided on a non-confidential basis to Company and Company is free to retain, disclose, use and incorporate such Feedback in Company's and/or its affiliates' products and services, without payment of royalties or other consideration to Customer. Customer understands and agrees that Company is not obligated to use, display, reproduce, or distribute any such Feedback, and that it has no right to compel such use, display, reproduction, or distribution. Nothing herein shall be interpreted as imposing an obligation on Customer to provide Feedback to Company.

(h) Certain items of software used in the Services are subject to "open source" or "free software" licenses ("Open Source Software"). Some of the Open Source Software is owned by third parties. The Open Source Software is not subject to the terms and conditions of Sections 2(a) or 4(a). Instead, each item of Open Source Software is licensed under the terms of the end-user license that accompanies such Open Source Software. Nothing in this Agreement limits Customer's rights under, or grants Customer rights that supersede, the terms and conditions of any applicable end user license for the Open Source Software. If required by any license for particular Open Source Software, Company makes such Open Source Software, and Company modifications to that Open Source Software, available by written request at the notice address specified on the Order Form.

3. Privacy and Security

(a) Company maintains appropriate administrative, technical and physical security measures to protect User Data to the extent reasonably necessary for the performance of the Services consistent with all applicable state and federal laws and regulations. In the event Company becomes aware of a breach or suspected breach of any privacy or security measures that compromises the confidentiality or integrity of data that is linked to or can be linked to an identifiable individual ("Personal Data"), Company will promptly notify Customer thereof, and use commercially reasonable efforts to remedy such breach.

(b) The parties agree that Customer is an educational institution, that Company is a service provider to Customer, and that Company's collection and use of the personally identifiable User Data of children under the age of 18 ("Minor User Data") is conducted on behalf of and with the authorization of Customer, in order to provide the Services requested by Customer. Customer has received and reviewed Company's Privacy Policy, which includes a privacy policy and direct notice of privacy practices as required by the Children's Online Privacy Protection Act Rule, 16 C.F.R. 313 ("COPPA"). Customer expressly consents to the collection, use and disclosure of Minor User Data as set forth in the Privacy Policy as applicable to those Services requested by Company. For the purposes of COPPA, Customer acknowledges that it is an educational institution, that it plans to use the Services in its capacity as an educational institution, and that it

is authorized to consent to the collection, use and disclosure of Minor User Data by Company in order to provide the Services. Customer further acknowledges, and Company agrees to provide, Customer an opportunity to review the Minor User Data, and to request that such data be corrected (to the extent practicable), deleted, and/or no longer collected or used (which may impact the availability of the Services). By using the Services, Customer expressly acknowledges that it has received and reviewed the Privacy Policy, and grants its consent to Company's collection, use and disclosure of Minor User Data in accordance with the Privacy Policy, which may be updated from time to time, provided Customer will be notified of any material changes. The Parties further agree that Company is a "school official" with a legitimate educational interest in receiving Personal Information about students. For the purposes of FERPA, Company agrees that it will comply with the requirements of 34 C.F.R. § 99.33 regarding its use and redisclosure of Educational Information (as defined in FERPA). Customer agrees and consents to the Company's use of such information so long as such use complies with FERPA. Customer acknowledges that it is responsible for notifying the Company that a student or parent objects to Company's use of Minor User Data in accordance with this Agreement.

(c) Notwithstanding Section 2(b), Customer expressly agrees that Company may aggregate or de-identify User Data, including Minor User Data, such that it no longer is linked or reasonably linkable to an identifiable individual ("De-Identified/Aggregated Data"), and may maintain and use such data for its own purposes as set forth in the Privacy Policy, provided it has implemented reasonable safeguards to prevent the re-identification of Aggregate Data.

(d) Customer agrees that Company may transfer User Data to its successor pursuant to a merger, consolidation or sale of substantially all of its assets pursuant to Section 15 of this Agreement and its successor may use, disclose, re-identify, store, or delete such data to the same extent that Company may do so pursuant to this Agreement.

4. Customer Responsibilities

(a) Customer agrees that it shall not, nor permit any User or other party to, do any of the following: (i) modify, make derivative works of, disassemble, reverse compile, or reverse engineer any part of the Services (including any Client Software), or in any way attempt to reconstruct or discover any source code or underlying ideas or algorithms of any part of the Services (including any Client Software); (ii) access or use the Services (including any Client Software) in order to build a similar or competitive product or service or for the purposes of bringing an intellectual property infringement claim against Company; (iii) except as otherwise expressly provided herein, copy, reproduce, distribute, republish, download, display, post or transmit in any form or by any means any of the Services (including any Client Software or any related documentation); (iv) attempt to gain unauthorized access to the Services and Customer shall make commercially reasonable efforts to prevent unauthorized third parties from accessing

the Services (including any Client Software); or (v) exceed the permitted number of devices, active users or students, teachers, faculty and staff in a school or district, in each case as specified in an Order.

(b) Customer agrees that it shall not, nor permit any User or other party to (i) access or attempt to access the administrative interface of the Services by any means other than through the interface that is provided by Company in connection with the Services, unless otherwise agreed in writing or (ii) intentionally engage in any activity that interferes with or disrupts the Services (or any servers or networks that are connected to the Services).

(c) Customer agrees that it is responsible for all activity occurring under Customers' accounts for the Services by its authorized users. Customer shall notify Company within a commercially reasonable time of any unauthorized use of any user account or any unauthorized use of the Services. Customer may not access the Company Services in a manner intended to avoid incurring fees or provide incorrect information for an Order for purposes of reducing amounts payable to Company. User IDs cannot be shared or used by more than one User at a time.

(d) If any software or documentation is acquired by or on behalf of a unit or agency of the United States Government, Customer agrees that such software or documentation is "commercial computer software" or "commercial computer software documentation" and that, absent a written agreement with Company to the contrary, Customer's rights with respect to such software and documentation are, in the case of civilian agency use, Restricted Rights (as defined in FAR §52.227.19), and, if for DoD use, limited by the terms of this Agreement, pursuant to DFARS §227.7202.

(e) Where Customer's use of the Services include visitor management, verification and tracking of visitors and other individuals, and related services or applications ("VMS"): agrees that: (i) it is responsible for ensuring that its collection, use and disclosure of all information (including personal information) and its instructions to Securly comply with applicable laws; (ii) it has provided (and will continue to provide) adequate notices and has obtained (and will continue to obtain) the necessary permissions and consents from each relevant individual to the collection, use, disclosure and/or storage of their information; (iii) it will not use the VMS (or any other of the Services) for the purposes of obtaining or conducting, background checks, employment verification, hiring, promotion, retention, termination, or reassignment decisions including but not limited to with respect to vendors, employees, contractors, providers, volunteers or other personnel; or otherwise engaging in any activities that are regulated by the Fair Credit Reporting Act (as amended) and the regulations, guidance, and orders promulgated thereto ("FCRA") or other state or federal laws or regulations related to consumer credit reports and background checks.

5. Confidential Information

(a) “Confidential Information” means any and all non-public information provided or revealed by one party (“Discloser”) to the other party (“Recipient”) or otherwise learned by a party during the course of performance under this Agreement, including without limit software, programs, prices, processes, documentation, financial, marketing and other business information, and all other material or information that is identified at the time of disclosure as confidential or proprietary or which otherwise would reasonably be expected to be kept confidential. Confidential Information shall also include: (i) the Discloser’s planned or existing computer systems and systems architecture, including computer hardware, computer software, source code, object code, documentation, methods of processing and operational methods; (ii) the Discloser’s customer lists, sales, profits, organizational structure and restructuring, new business initiatives and finances; (iii) the Discloser’s services and products, product designs, and how such products are administered and managed; and (iv) Customer’s User Data, including Minor User Data and Customer Personal Information. Recipient’s obligations of confidentiality shall not apply to information that: (1) is or becomes public through no fault or breach by Recipient, (2) is or becomes known to Recipient (either directly or rightfully through a third party) without an obligation of confidentiality, or (3) is independently developed by Recipient without use of or access or reference to Discloser’s Confidential Information.

(b) During the Term of this Agreement and for a period of five (5) years following the termination or expiration of this Agreement, or with respect to any Confidential Information that constitutes a trade secret of the Discloser, for so long as such information constitutes a trade secret, Recipient shall hold Discloser’s Confidential Information in confidence and will not disseminate or disclose the Confidential Information to any third party except its Personnel, as set forth herein, unless required by applicable law to do so. Recipient will protect Discloser’s Confidential Information with the same degree of care it uses to protect its own confidential information of a similar nature, but in no event will Recipient use less than a reasonable degree of care. Recipient will use Discloser’s Confidential Information solely to the extent necessary to exercise its rights and obligations under this Agreement and will ensure that Confidential Information is disclosed only to its employees, contractors and other personnel (individually and collectively, “Personnel”) with a bona fide need to know and who are under binding written obligations of confidentiality with Recipient to protect Discloser’s Confidential Information substantially in accordance with the terms and conditions of this Agreement. The Recipient shall be responsible for any breach of this Section 5 by any Personnel. In addition, Recipient will implement and maintain appropriate technical and organizational measures to protect Confidential Information against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the Confidential Information to be protected. Recipient may disclose Confidential Information to the limited extent required to by the order or requirement of a court, administrative agency, or other governmental body; provided, however, that the Recipient notifies the Discloser in writing

in advance of such disclosure (unless prohibited by law from doing so) and provides the Discloser with copies of any related information so that the Discloser may take appropriate action to protect its Confidential Information.

(c) All Confidential Information is and shall remain the sole property of Discloser, and Recipient shall not acquire any rights or licenses therein except as expressly set forth in this Agreement. Recipient shall return to Discloser (or at Discloser's option, destroy) any and all Confidential Information and any other information and materials that contain such Confidential Information (including all copies in any form) immediately upon Discloser's written request, when the Information is no longer required to provide the services, and upon the termination of this Agreement, in each case in accordance with Receiver's written data retention and destruction policies. Within ten (10) days following Discloser's written request, Recipient will provide Discloser with a written certification, as signed by an officer or executive level employee of Recipient, certifying compliance with this Section 5. For the avoidance of doubt, Recipient shall not be required to return or destroy Aggregate Data.

(d) Recipient acknowledges that the disclosure of Confidential Information in breach of the terms of this Section 5 may cause Discloser irreparable injury and damages that may be difficult to ascertain. Therefore, Discloser, upon a disclosure or threatened disclosure of any Confidential Information by Recipient or any Personnel, will be entitled to injunctive relief (without being required to post bond), including, but not limited to, a preliminary injunction upon an ex parte application by the Discloser to protect and recover its Confidential Information, and the Recipient will not object to the entry of an injunction or other equitable relief against the Discloser on the basis of an adequate remedy at law, lack of irreparable harm or any other reason. Without limiting the foregoing, the Recipient will advise the Discloser immediately in the event that it learns or has reason to believe that any person or entity that has had access to Confidential Information, directly or indirectly, through the Receiver, has violated or intends to violate the terms of this Agreement. This provision will not in any way limit such other remedies as may be available to the Discloser, whether under this Agreement, at law, or in equity.

6. Billing and Payment

(a) The amount of the recurring fees associated with the use of the Services and the Support Services by Customer shall be as set forth in the Order (the "Fees"). Fees for Services may be charged based on the number of (i) devices or active Users, (ii) the number of students in a school or district, or (iii) students, teachers, faculty and staff in a school or district, as specified in an Order. Additionally, there may be other basis for calculating the Fees, as specified in the Order. The Fees exclude all applicable sales, use, and other taxes, fees, duties and similar charges ("Taxes"), and Customer will be responsible for payment of all such Taxes (other than taxes based on Company's income) and any penalties or charges that accrue with respect to the

non-payment of any Taxes as well as government charges, and all reasonable expenses and attorneys' fees Company incurs collecting late amounts. All amounts payable under this Agreement will be payable in U.S. Dollars within thirty (30) days of receipt of invoice, unless specified otherwise in the Order or Customer is purchasing the Services and Support Services through an authorized reseller and the parties have agreed that Customer is to pay the authorized reseller directly. Payment of fees shall be made by the Customer prior to receiving the Services. The payment may be made by check or wire transfer. Unless prohibited by applicable law, late payments may bear interest at the rate of 1.5% per month (or the highest rate permitted by law, if less). To the fullest extent permitted by law, Customer waives all (i) claims relating to charges unless claimed within sixty (60) days after invoicing, and (ii) refunds under any situations aside from those contemplated in this Agreement. Notwithstanding any fees for services posted on Company's website or otherwise published by Company, the parties acknowledge and agree that the Fees may only be modified as set forth below in the "Modification; Waiver" section of this Agreement.

(b) If Customer is purchasing the Services or Support Services (or both) through an authorized reseller, Customer shall pay the fees for the Services and Support Services, as applicable, on a timely basis directly to the authorized reseller. Without limiting Company's remedies under this Agreement, at law or in equity, Company reserves the right to suspend provision of the Services or Support Services (or both) and to terminate this Agreement should Customer fail to pay the authorized reseller on time, regardless of the reason.

7. Term and Termination

(a) This Agreement commences on the Effective Date and, unless terminated earlier in accordance with this Agreement, shall remain in effect for the initial period specified in the Order (or, if no period is specified in the Order, then for an initial period of twelve (12) months) (the "Initial Term"). Unless otherwise specified in an agreement containing the Customer Terms, this Agreement will thereafter continue for successive twelve (12) month periods (each, a "Renewal Term"), unless either party gives the other party written notice of non-renewal at least 30 days prior to the end of the then-current term. The Initial Term, together with all Renewal Terms, are collectively referred to as the "Term". Unless a fixed term without renewals is specified in a Services Agreement, it is Customer's responsibility to provide timely notice of non-renewal as required herein, and failure to do so will result in automatic renewal of the Agreement.

(b) Either party may terminate this Agreement by giving written notice to the other party upon the occurrence of an Event of Default by the other party. For purposes of this Agreement, "Event of Default" means a breach by a party of any of its representations, warranties, or obligations under this Agreement, if such breach remains uncured for a period of thirty (30) days following receipt of written notice from the other party.

(c) If Customer is a government entity, Customer may terminate this Agreement upon advance written notice provided at least thirty (30) days prior to the end of the then-current term in the event that funds are not appropriated for any renewal year.

(d) Customer may terminate this Agreement for convenience upon thirty (30) days advance written notice; provided, however, in the event of a termination for convenience Customer shall not be entitled to a pro rata refund of fees paid or reduction in fees owed for the then current term.

(e) Any and all provisions in this Agreement that would reasonably be expected to be performed after the termination or expiration of this Agreement shall survive and be enforceable after such termination or expiration, including without limitation provisions relating to confidentiality, ownership of materials, payment, taxes, representations and warranties, indemnification, limitations of liability, effects of termination, and governing law.

(f) Immediately upon termination of this Agreement, (a) the licenses granted to either party shall immediately terminate; and (b) Company shall cease to make available and Customer shall cease to use the Services. Termination shall not relieve Customer's obligation to pay all charges accrued before the effective date of termination.

8. Representations and Warranties

(a) Each party represents, covenants, and warrants to the other party that there is no applicable law, regulation, rule, or other governmental requirement that: (i) in any way restricts or limits the duty of party to fully perform and comply with all obligations set forth in this Agreement; or (ii) impairs the rights of the other party as set forth in this Agreement;

(b) Company represents, covenants, and warrants that it will provide the Services (i) in all material respects as described in the applicable end user documentation, if any, (ii) in a professional manner and in accordance with generally accepted industry practices, and (iii) in compliance with all applicable laws and regulations. If the Services provided to Customer are not performed as warranted, Customer agrees that it must promptly provide a written notice to Company that describes the deficiency in the Services.

(c) Company represents, covenants, and warrants that the Services will not (i) infringe any copyright, trademark, or patent right; or (ii) misappropriate any trade secret.

(d) Customer represents, covenants, and warrants that it will use the Services only in compliance with the terms and conditions of this Agreement and all applicable laws and regulations and that Customer's content shall not (i) infringe any copyright, trademark, or patent

right; (ii) misappropriate any trade secret; (iii) be deceptive, libelous, obscene, pornographic or unlawful; (iv) contain any viruses, worms or other malicious computer programming codes intended to damage Company's system or data; or (v) otherwise violate any privacy or other right of any third party. Although Company has no obligation to monitor Customer's use of the Services, Company may do so and may prohibit any use of the Services it reasonably believes may be (or is alleged to be) in violation of this Agreement or applicable laws and regulations.

(e) If Customer is a government entity, unit, agency, organization, entity or party (including a school or school district), then Customer represents, warrants and covenants that Customer has taken all actions, complied with all requirements, obtained all prior consents and reviews, and otherwise satisfied all prerequisites that may be necessary or appropriate to enable Customer to enter into and perform this Agreement in accordance with its terms and conditions.

(f) Where Customer uses the Services to send emergency notifications, alerts or other messages to recipients, including via text/SMS, phone, prerecorded message, email or other electronic communication ("Electronic Communication"), Customer represents, warrants and covenants that: (i) it has provided (and will continue to provide) adequate notices and has obtained (and will continue to obtain) the necessary permissions and consents from each recipient to receive such Electronic Communications from or on behalf of Securly, including as required by the Telephone Consumer Protection Act ("TCPA") and the CAN-SPAM Act, each as amended and including the regulations, guidance, and orders promulgated pursuant to such each; (ii) it will not send any Electronic Communication to a recipient that has not consented to receive such communications from Customer; (iii) it will not send any Electronic Communication to any recipient that has specifically opted out of receiving Electronic Communications from Company; (iv) not send, direct Securly to send or otherwise direct or cause to be sent any Electronic Communication in violation of applicable law or this Section 8(f); (v) it will maintain adequate records of consents and its compliance with this Section 8(f) and shall provide upon request any such records to Securly for inspection; and (vi) it will only send, direct to be sent or otherwise cause to be sent Electronic Messages to (A) students, parents, guardians, personnel and other authorized parties, and (B) only for emergency purposes (as defined pursuant to the TCPA).

(g) Customer represents, warrants and covenants that the software for the Services provided under this Agreement will be treated as "commercial computer software" and "commercial computer software documentation" under any applicable governmental laws, regulations or rules.

9. Disclaimers, and Exclusive Remedies

(a) COMPANY DOES NOT GUARANTEE THAT (A) THE SERVICES WILL BE PERFORMED ERROR-FREE OR UNINTERRUPTED, OR THAT COMPANY WILL CORRECT ALL ERRORS, (B) THE SERVICES WILL OPERATE IN COMBINATION WITH CUSTOMER'S CONTENT OR APPLICATIONS, OR WITH ANY OTHER HARDWARE, SOFTWARE, SYSTEMS, SERVICES OR DATA NOT PROVIDED BY COMPANY, AND (C) THE SERVICES WILL MEET CUSTOMER'S OR ITS USERS' NEEDS, REQUIREMENTS, SPECIFICATIONS, OR EXPECTATIONS. CUSTOMER ACKNOWLEDGES THAT COMPANY DOES NOT CONTROL THE TRANSFER OF DATA OVER COMMUNICATIONS FACILITIES, INCLUDING THE INTERNET, AND THAT THE SERVICES MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF SUCH COMMUNICATIONS FACILITIES. COMPANY IS NOT RESPONSIBLE FOR ANY ISSUES RELATED TO THE PERFORMANCE, OPERATION OR SECURITY OF THE SERVICES THAT ARISE FROM CUSTOMER'S CONTENT OR APPLICATIONS, OR THIRD PARTY CONTENT (INCLUDING PUBLICLY AVAILABLE DATA OR OTHER THIRD PARTY DATA) OR SERVICES, AND DISCLAIMS ALL LIABILITIES ARISING FROM OR RELATED TO THIRD PARTY CONTENT OR SERVICES.

(b) NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THIS AGREEMENT, COMPANY DOES NOT GUARANTEE OR WARRANT (A) THAT THE SERVICES WILL FUNCTION TO PREVENT MINORS FROM BEING EXPOSED TO INAPPROPRIATE, HARMFUL, UNSAFE, OR OBSCENE CONTENT ONLINE, (B) THAT THE SERVICES WILL FULFILL CUSTOMERS OBLIGATIONS, IF ANY, UNDER THE CHILDREN'S INTERNET PROTECTION ACT, (C) THAT THE SERVICES WILL PREVENT OR OTHERWISE DISCOURAGE CYBERBULLYING OR SELF HARM BY STUDENTS, (D) THAT THE SERVICES WILL DETECT ALL CYBERBULLYING AND SELF-HARM BY STUDENTS, OR (E) ALL SOCIAL MEDIA SITES, STREAMING MEDIA, WEB BASED EMAIL SERVICES, CLOUD STORAGE SITES, OTHER INTERNET SITES (INCLUDING PORN, GAMBLING AND OTHER INAPPROPRIATE SITES FOR MINORS), DIRECT MESSAGES AND ELECTRONIC DOCUMENTS AND FILES WILL BE BLOCKED OR MONITORED OR (F) THE ACCURACY OR RELIABILITY OF ANY INFORMATION OBTAINED THROUGH THE SERVICES INCLUDING BUT NOT LIMITED TO AND THIRD PARTY DATA OR THE RESULTS OF ANY QUERIES OR SEARCHES SUBMITTED BY CUSTOMER FOR PURPOSES OF SCREENING VISITORS, OR (G) THE SERVICES WILL DETECT OR PREVENT FROM ENTERING SCHOOL PREMISES ANY OR ALL INDIVIDUALS THAT ARE UNAUTHORIZED OR OTHERWISE PROHIBITED BY APPLICABLE LAW OR CUSTOMER POLICY FROM ENTERING OR VISITING CUSTOMER PREMISES OR PROPERTY.

(c) FOR ANY BREACH OF THE SERVICES WARRANTY, CUSTOMER'S EXCLUSIVE REMEDY AND COMPANY'S ENTIRE LIABILITY SHALL BE THE CORRECTION OF THE DEFICIENT SERVICES THAT CAUSED THE BREACH OF WARRANTY, OR, IF COMPANY CANNOT SUBSTANTIALLY CORRECT THE DEFICIENCY IN A COMMERCIALY

REASONABLE MANNER (AS DETERMINED SOLELY BY COMPANY IN ITS REASONABLE DISCRETION), THEN CUSTOMER MAY TERMINATE THE SERVICES AND COMPANY WILL REFUND TO CUSTOMER THE FEES FOR THE TERMINATED SERVICES THAT CUSTOMER PRE-PAID TO COMPANY FOR THE PERIOD FOLLOWING THE EFFECTIVE DATE OF TERMINATION. IN SUCH AN EVENT, COMPANY SHALL ALSO EXERCISE COMMERCIALY REASONABLE EFFORTS TO PROVIDE CUSTOMER WITH REASONABLE OPPORTUNITY TO ACCESS THE SERVICES FOR THE PURPOSES OF SECURING AND BACKING UP CUSTOMER'S USER DATA.

(d) TO THE EXTENT NOT PROHIBITED BY LAW, THESE WARRANTIES ARE EXCLUSIVE AND THERE ARE NO OTHER WARRANTIES, AND COMPANY HEREBY DISCLAIMS AND EXCLUDES ALL OTHER WARRANTIES, WHETHER STATUTORY, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE.

10. Limitation of Liability

BOTH PARTIES EXPRESSLY UNDERSTAND AND AGREE THAT NEITHER PARTY SHALL BE LIABLE TO THE OTHER UNDER THIS AGREEMENT FOR ANY INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, LOSS OF TIME OR LOST PROFITS) ARISING OUT OF, OR IN ANY WAY CONNECTED WITH THIS AGREEMENT, EVEN IF SUCH PARTY HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. WITH THE EXCEPTION OF WILLFUL OR GROSSLY NEGLIGENT BREACHES OF SECTION 5, AND WITHOUT AFFECTING THE LIMITATIONS OF LIABILITY SET FORTH IN SECTION 10, IN NO EVENT SHALL COMPANY'S AGGREGATE LIABILITY OF ANY TYPE UNDER THIS AGREEMENT EXCEED THE AMOUNTS ACTUALLY PAID BY AND/OR DUE FROM CUSTOMER IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH CLAIM REGARDLESS OF THE FORM OF ACTION, WHETHER BASED ON CONTRACT, TORT, WARRANTY, NEGLIGENCE, STRICT LIABILITY, PRODUCTS LIABILITY OR OTHERWISE. THIS PARAGRAPH DOES NOT APPLY TO CUSTOMER'S VIOLATION OF COMPANY'S INTELLECTUAL PROPERTY RIGHTS.

11. Indemnification

(a) Customer Obligations. To the extent permitted under applicable law, Customer shall defend Company against any claim, cause of action, suit or proceeding (each a "Claim") made or brought against Company by a third party arising out of or attributable to Customer's use of the Service (other than as expressly set forth in Section 11(b) below), and shall indemnify Company

for any damages finally awarded against, and for reasonable attorney's fees incurred by, Company in connection with the Claim, on condition that Company (a) promptly gives Customer written notice of the Claim; (b) gives Customer sole control of the defense and settlement of the Claim (provided that Customer may not settle any Claim unless the settlement unconditionally release Company of all liability); and (c) provides reasonable assistance in connection with the defense (at Customer's reasonable expense).

(b) Company Obligations. Company shall defend Customer against any Claim made or brought against Customer by a third party: (i) to the extent arising out of Company's gross negligence and/or willful misconduct; or (ii) alleging that Customer's use of the Service infringes or misappropriates the intellectual property rights of a third party, and shall indemnify Customer for any damages finally awarded against, and for reasonable attorney's fees incurred by, Customer in connection with the Claim. If a Claim is brought or threatened, or Company believes is likely to occur, Company may, at its option, (i) procure for Customer the right to use the Service, (ii) replace the Service with other suitable products, or (iii) refund any prepaid fees that have not been earned and terminate this Agreement upon notice. Company will have no liability under this Agreement or otherwise to the extent a Claim is based upon (a) use of the Service in combination with software, hardware or technology not provided by Company, if infringement would have been avoided in the absence of the combination, (b) modifications to the Service not made by Company, if infringement would have been avoided by the absence of the modifications, (c) use of any version other than a current release of the Service, if infringement would have been avoided by use of a current release, or (d) any action or omission of Customer for which Customer is obligated to indemnify Company under this Agreement. This Section 11(b) states the Company's sole liability to, and the Customer's exclusive remedy against, the Company for any type of intellectual property infringement claim.

(c) Conditions of Indemnification. The indemnifications provided in this Agreement are conditioned on the indemnified party: (i) promptly giving the indemnifying party written notice of the Claim; (b) giving the indemnifying party sole control of the defense and settlement of the Claim (provided that the indemnifying party may not settle any Claim unless the settlement unconditionally release indemnified party of all liability); and (c) provides reasonable assistance in connection with the defense (at the indemnifying party's reasonable expense).

12. Advertising and Public Announcements

Neither party will use the other party's name or marks, refer to or identify the other party in any advertising or publicity releases or promotional or marketing correspondence to others without such other party's written approval. Notwithstanding the foregoing, Company may publish Customer's name as part of a publicly-available list of Company's customers.

13. Relationship of the Parties

The parties are independent contractors with respect to each other, and nothing in this Agreement shall be construed as creating an employer-employee relationship, a partnership, fiduciary, or agency relationship or any association or joint venture between the parties. Neither party is, nor will hold itself out to be, an agent of the other party. Neither party is authorized to enter into any contractual commitment on behalf of the other party.

14. Force Majeure

Except for payment obligations already due and owing, any delay in or failure of performance by a party under this Agreement will not be considered a breach of this Agreement and will be excused to the extent caused by any occurrence beyond the reasonable control of such party, provided that the party affected by such event will immediately notify the other party and begin or resume performance as soon as practicable after the event has abated. If the act or condition beyond a party's reasonable control that prevents such party from performing any of its obligations under this Agreement continues for thirty (30) days or more, then the other party may terminate this Agreement immediately upon written notice to the non-performing party. Without limitation, act or condition beyond Company's reasonable control include all acts and omissions of Company's service providers. In the event of such termination by Customer, Company shall refund to Customer such fees for the terminated services that Customer pre-paid to Company for the period following the effective date of termination, and shall also exercise commercially reasonable efforts to provide Customer with reasonable opportunity to access the Services for the purpose of retrieving User Data. In all other instances of delay or failures on the part of Company under this Section 14 (i.e. wherein Customer does not or otherwise cannot terminate this Agreement pursuant to this Section 14), Customer shall not be entitled to any service credit or refund.

15. Binding Effect; Assignment; Third Parties

The terms and conditions of this Agreement shall be binding on the parties and all successors and permitted assigns of the foregoing. Company may assign or transfer, by operation of law or otherwise, any or all of its rights, burdens, duties or obligations under this Agreement in connection with a merger, acquisition, sale of substantially all of its assets, or other corporate transaction, provided that such assignee has assumed in writing all of Company's obligations under the Agreement and agreed to be bound by all the terms and conditions of the Agreement accruing or arising from and after the effectiveness of such assignment. Company will notify Customer in writing within ninety (90) days of any such change of control. To the extent the assignee is an entity prohibited from conducting business in the State in which the Customer is established, the Customer will have the option to terminate the Agreement. This Agreement is

intended for the sole and exclusive benefit of the parties, is not intended to benefit any third party, and only the parties may enforce this Agreement.

16. Modification; Waiver

All modifications to or waivers of any terms and conditions of this Agreement (including any exhibit) must be in a writing that is signed by the parties hereto and expressly references this Agreement. No waiver of any breach of any provision of this Agreement shall constitute a waiver of any prior, concurrent or subsequent breach of the same or any other provisions hereof, and no waiver shall be effective unless made in writing and signed by an authorized representative of the waiving party.

17. Governing Law

This Agreement and all actions arising out of or in connection with this Agreement shall be construed under and governed by and interpreted in accordance with the laws of the State in which Customer is established, without regard to the conflicts of law provisions thereof.

18. Export Control

The use of the Services is subject to U.S. export control laws and may be subject to similar regulations in other countries.

19. Severability

In the event that any provision of this Agreement shall be held invalid, illegal, or unenforceable by a court with jurisdiction over the parties to this Agreement, such invalid, illegal, or unenforceable provision shall be deleted from the Agreement, which shall then be construed to give effect to the remaining provisions thereof.

20. Notices

All notices, consents and approvals under this Agreement must be delivered in writing by personal delivery, courier, express mail service, or by certified or registered mail, (postage prepaid and return receipt requested) or by e-mail, with reasonable confirmation of receipt, to the other party at the address set forth on at the beginning of this Agreement (in the case of Company) or the Order (in the case of Customer), or such other address as a party may designate from time to time by written notice to the other party. Notice given by mail shall be

effective five (5) days after the date of mailing, postage prepaid and return receipt requested. Notice by personal delivery, courier service, or express mail service shall be effective upon delivery.

21. Interpretation

SB

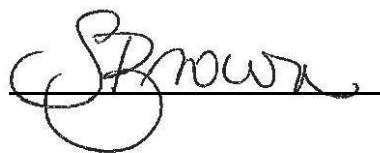
This Agreement may be executed in counterparts, each of which will constitute an original, and all of which will constitute one agreement. The section headings and captions in this Agreement are for convenience of reference only and have no legal effect. If there is a conflict or ambiguity between this Agreement and the Order, the terms and conditions of the Order, **into which the attached University Laboratory School Software addendum is hereby incorporated**, shall control.

22. Entire Agreement

SB

This Agreement, **including the attached University Laboratory School Software Addendum**, and the Privacy Policy constitute the entire agreement between the parties with respect to the subject matter hereof and supersede all prior and contemporaneous oral or written representations, agreements or communications, including, without limitation, any quotations or proposals submitted by Company that are not shown in the Order or any policies or terms for the Services posted on www.securly.com other than the Privacy Policy.

The Board of Trustees of Illinois State University

A handwritten signature in cursive script, appearing to read "C. Brown", written over a horizontal line.

Securly, Inc.

A handwritten signature in cursive script, appearing to read "End", written over a horizontal line.

Privacy Policy

Last updated: Aug 14, 2024

Securly, Inc. (“Securly,” “we,” “our” or “us”) recognizes the importance of privacy. This Privacy Policy describes how we collect, store, use and disclose, or otherwise process (collectively “process”) information, including personal information.

Securly Collects different information about different types of users and uses that information for different purposes, as described in this Privacy Policy. If you are a Student, Parent, or Educator, see Section 1 for a description of the processing of data collected through Securly’s software products and services (“Services”). If you are an adult visiting our website, see Section 2 for a description of the processing of data collected through Securly’s website, www.securly.com (the “Site”).

Section 1: For Students, Parents, and Educators using our Services

How Securly processes information collected through our Services

This section of the Privacy Policy covers data from Students, Parents, and Educators as they interact with Services, including

- Cloud-based web filtering (such as Filter);
- cyber-bullying and self-harm detection (such as Aware and Observe);

- Student wellness monitoring tools (such as Rhithm);
- AI generated data analysis (such as Discern);
- digital classroom management tools (such as Classroom, Pass, Flex, and Visitor);
- at School and take-home policies for School issued devices (such as MDM); and
- the Parent mobile app (such as Home)

Additionally, this policy covers all Services previously offered by Rhithm and Eduspire Solutions that link to this Policy.

When Securly's customers—schools, districts, or other educational institutions that are its customers (collectively "Schools")—install and use Securly Services, we collect information about the Schools' students ("Students") and their parents or guardians ("Parents"), as well as teachers, officials, and other School employees (collectively "Educators").

Information collected via the Services, is processed by Securly as a data processor or service provider on behalf of Schools. The Schools are the controllers of any personal information collected through the Services. This information will be treated in accordance with this section of this Privacy Policy as well as our Terms of Use and is also subject to the policies and practices of the School on whose behalf we are processing the information.

To provide the Services for which Schools contract with us, Securly collects personal information from Students for the sole use and benefit of the Students and the School in the educational context as authorized by Schools, and for no other commercial purpose.

a. Applicable Federal Law

We are committed to complying with the Federal Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part 99), the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506, in all applicable respects with regard to the collection, use, disclosure, and retention of Student Information.

FERPA

Under FERPA, when Schools contract for Securly Services, Securly functions as a School Official, which has a legitimate educational interest in Students' education records. In accordance with FERPA, Securly (i) performs an institutional service or function for which the School would otherwise use employees; (ii) remains under the direct control of the School regarding the use and maintenance of education records; and (iii) agrees to use Student Information from education records only for the purposes for which the disclosure was made, e.g., to promote School safety and the physical security of Students, and will not disclose

Student Information from education records for any other purpose. “Student Information” includes any information about a Student that is linked to that Student’s identity. Anonymized and aggregated Student data is not Student Information.

COPPA

Under COPPA, parental consent is required to collect personal information online from children under 13. When Schools use our Services, the School consents on behalf of Parents to the collection and use of personal information from Students as part of signing up to use the Services.

b. Consent

By contracting for the Services, Schools provide consent for Securly to collect and use personal information, anonymous information, and aggregate information about Students as a School Official on behalf of the School. Schools are responsible for confirming that they are authorized to consent to the collection and use of this information and to obtain any necessary consents from the Parent or Student.

In order to use Securly Services, Schools must consent to the collection and use of Student Information Use of the Services, and any dispute over privacy, is subject to this Policy and our Terms of Service including its applicable limitations on damages and resolution of disputes. This Policy is incorporated by reference into the [Terms of Service](#).

Student Information will not be used for any purpose unrelated to the provision the Services without consent. Securly may, however, use aggregated or anonymized Student data for the improvement of its Services. Consent for the processing of Student Information may be withdrawn by a School, Parent, or eligible Student at any time. However, withdrawing consent may result in Students’ inability to continue using some or all of the Services.

Parents and Educators who are adult users of the Services consent to collection of their own personal information through their use of the Services.

c. Types of Information Collected by the Services

The Services may collect information directly from Schools, Students, Parents, Educators, third parties, and directly from use of the Services. Such information may include, but is not limited to, Student Information, which includes identifiable information about the Student’s online activity, social media usernames and activity, electronic communications, and general web browsing activity.

Information the Services Collect Directly

When the Services are used, we collect Students' mobile device ID; device name and model; and operating system type, name, and version of School issued devices.

Information the Services Collect Automatically

In order to provide our Services and to understand a Student's activity while using our Services, we may automatically collect the following information about a Student through cookies, web beacons, and other technologies: information regarding a Student's personal computing device, browser type, browser language, operating system, Internet Protocol ("IP") address, and the actions a Student takes while using the Services including while online (such as the web pages viewed or blocked, the length of time a Student visited a website, links clicked, and messages sent or posted).

When Students use the Services on a personal computing device, we may use geolocation information to determine their current location. Such information is specific to the device only and is not specific to any Student. We may also use elements of a Student's usage and analytics information (such as IP address) to determine their generalized location.

Student Information Collected from Social Networking Sites

If Students use Facebook, X, or other social networking sites, Securly will collect Students' activity on those sites ("Social Networking Activity"), including posts to Students' Facebook, Twitter, or Google+ accounts, and other messaging activity for purposes of providing the Services, including, as applicable, for detection of cyber-bullying or self harm protection. Securly will collect Students' Social Networking Activity even if Students have chosen not to make that activity public. We store Students' Social Networking Activity with other information that we collect from Students.

d. How the Services Use Student Information

We use Student Information in the following ways:

- To provide Services to Schools including to respond to customer service and technical support issues and requests. If a Student runs into technical errors while using the Services, we may request School permission to obtain a crash report along with certain logging information from the computing device utilized by the Student documenting the error. This may include information regarding the device's Operating System version, hardware, and browser version (and .NET version information in case of Windows systems).

- To log Students' online activities on behalf of Schools, including the information a Student distributes, displays, or shares, to provide Schools and Parents with alerts, reports, and logs regarding the same. Such reports may include class or School-wide Student activity reports, to allow Schools to conduct comparative analyses of Students.

We do not use Student Information in the following ways:

- We do not collect Student Information for the purpose of sale of such information in any way or for building commercial Student profiles, or for any other commercial purposes not related to the provision of the Services.
- We do not use Student Information for advertising.

We may use aggregate or de-identified Student Information for the following purposes:

- To monitor and analyze the Services and for technical administration;
- To better understand how Students access and use our Services;
- To improve and analyze our Services, such as by refining the types of activities that trigger (or do not trigger) an alert; and
- For other research and analytical purposes related to the Services.

e. How the Services Share Student Information

Service Providers. We may disclose Student Information to third-party vendors, service providers, contractors, or agents (collectively "Service Providers") who perform contractually defined functions on our behalf. We may engage Service Providers to perform Services (e.g., hosting) that may involve their access, use or storage of Student Information on our behalf. Service Providers have limited access to databases of Student Information solely for the purpose of helping us provide the contracted Services, and we have put in place contractual and other organizational safeguards requiring them to take steps to ensure a proper level of protection for Student Information. These third parties are contractually bound to treat Student Information in accordance with our privacy and security policies and commitments. Except as explained above, we do not disclose or transfer Student Information to third parties except for authorized educational/School purposes or as directed by the Schools that have engaged us to provide Services. We prohibit Service Providers from using Student Information for any purpose other than providing the contracted service.

Business Transfers. If we are acquired by or merged with another company, if substantially all of our assets are transferred to another company, or as part of a bankruptcy proceeding, we may transfer Student Information we have collected to the other company, provided the successor

entity is subject to equivalent privacy and security commitments as Securly and the information disclosed continues to be used for only educational/school purposes.

In Response to Legal Process. We may disclose Student Information to comply with the law, a judicial proceeding, court order, subpoena, or other legal process. In particular, many states have laws that require specific categories of persons, or any person, to report certain matters pertaining to child safety to relevant state or local authorities. These matters may include any reasonable suspicion of child abuse or neglect or the presence of child sexual abuse material. We may therefore be required by law to report information from certain alerts to relevant state or local authorities in these states.

To Protect Us and Others. We also may disclose Student Information where we believe it is necessary to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety of any person, violations of our Terms of Service or this Student Policy, or as evidence in litigation in which Securly is involved.

With Schools and Parents. In compliance with COPPA and FERPA, Schools and Parents are able to log in to view information about their Students' use of certain Services.

Aggregate and De-Identified Information. We may also use and share aggregate or de-identified information about students or children with third parties for research and analytical purposes.

f. Information Students Share with Third Parties

Students may be able to voluntarily share their Student Information with third parties, including Social Networking Activity, while using the Services. The privacy policies of these third parties are not under our control and may differ from ours. The use of any information that Students may provide to third parties will be governed by the privacy policy of such third party or by your independent agreement with such third party, as the case may be. Please consult their respective privacy policies. We have no control over how any third-party site uses or controls the information that it collects directly from Students.

g. Security of Student Information

The security of Student Information is important to us. We have implemented a security program that is reasonably designed to protect the Student Information we collect from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. We have implemented technical, contractual, administrative, and physical security steps and other organizational safeguards designed to protect personal information. This includes the use of authentication technologies, encryption where appropriate, and a securely configured network.

We have implemented procedures limiting the dissemination of Student Information to such designated Service Providers and Securly employees only as are reasonably necessary to carry out that Service Provider's or employee's specific role.

Please be aware that despite our best efforts, no data security measures can guarantee 100% security. You should take steps to protect against unauthorized access to your password, phone, and computer by, among other things, signing off after using a shared computer, choosing a robust password that nobody else knows or can easily guess, and keeping your log-in and password private. We cannot guarantee that our Services will always be perfectly secure, and we are not responsible for any lost, stolen, or compromised passwords or for any activity on your account via unauthorized password activity.

If we learn of a security breach that undermines the integrity and confidentiality of Student Information, we will notify affected customers in accordance with applicable law, contractual obligations, and industry practices. With the school's permission, we may also post a notice on the Securly website or elsewhere on the Service. Depending on the jurisdiction, affected teachers and students may be entitled by law to receive a written notice of a security breach.

h. Your Rights to Review, Delete and Control Our Use of Student Information

We will make reasonable efforts to keep Student Information accurate and up-to-date, and we will provide Students, Parents, and Educators with mechanisms to review, update, and correct Students' personal information as appropriate and/or desired.

Schools will control the Student Information we have collected and have all rights to review it, to delete it, and to tell us to no longer use it.

Notwithstanding the foregoing, Student Information will be deleted in all cases, including personal information held by our Service Providers, when a School instructs us that it is no longer needed for the purpose for which it was collected. All retained Student Information will remain subject to the terms of this Policy.

If we learn we have collected personal information about a Student without proper consent, we will delete that information as quickly as possible.

You can make a request to exercise Student Data rights by contacting us at support@securly.com or calling 1 (855) 732-8759 (ext. 101). We will review your request and respond accordingly.

i. Securly Classroom

Securly Classroom imports data using Google APIs to make the data available to Students and Educators through the Securly Classroom application. Chrome OS data is imported to allow Students and Educators to view and manage Chrome devices. Domain information is imported (OU list) to display and allow Schools to move devices between OUs and activate Lost Mode in Securly Classroom. User profile data is imported to provide class roster information to teachers and recognize Students based on their email address. User profile data also provides user photos in Securly Classroom. Classroom APIs are accessed to provide roster information and to allow teachers to access Classwork for use in managing classes.

The sole purpose for accessing all data from the Google domain is to provide the Securly Services to the School. No data is shared with any outside organization for any reason. The data is used exclusively to provide Schools the management services of the Securly products to which they subscribe.

Securly Classroom does not transfer information received from Google APIs to any application outside of products that are part of Securly's integrated suite of applications. The use of all information received through the APIs will adhere to the Google API Services user Data Policy, including the Limited Use requirements.

j. Securly Filter

Securly Filter uses YouTube APIs to enable schools and parents to see titles and thumbnails of YouTube URLs for videos or channels. To the extent schools permit Students to access YouTube content, Students may be sharing personal information with YouTube. YouTube's collection and use of that data is subject to YouTube's Terms of Service (<https://www.youtube.com/t/terms>) and the Google Privacy Policy at <http://www.google.com/policies/privacy>. As explained in section f. above, we have no control over how YouTube uses the information that it collects directly from Students.

k. Parent and Educator Data

To the extent that Parents or Educators interact with the Services, we may collect some minimal personal information about those individuals. This information is often combined with Student Information and is typically limited to name and contact information.

We may use information about Parents or Educators to communicate about your account and use of our Services. Parents or Educators who opt-out of receiving emails about

recommendations or other information may still receive transactional e-mails, such as about your account or any services you have requested or received from us.

Section 2: For adults visiting the Securly Site

How Securly processes information collected through our Site

This Section of the Privacy Policy describes how Securly collects and processes data from adults who interact with our Site. Nothing in this Section of the Privacy Policy describes the processing of Student data. For the purposes of this Privacy Policy, visitors to the Site are referred to as Site Visitors.

Site Visitors are adults. The Site is not directed to children under the age of 18, and we do not knowingly collect personal information from children under the age of 18 on the Site. If we discover that we inadvertently collected information from a child under the age of 18 through the Site, we will promptly delete it. By visiting our Site, Site Visitors acknowledge that you have been given this notice about how your information, including personal information, will be handled as described in this Policy. Your use of the Site, and any dispute over privacy, is subject to this Policy and our Terms of Use including any applicable limitations on damages and resolution of disputes. The Terms of Use are incorporated by reference into this Policy.

We process Site Visitors' personal information as set forth in this Section of the Privacy Policy or otherwise with Site Visitors' consent or as permitted or required by law. We base our processing of Site Visitors' personal information on consent, Site Visitors may withdraw your consent at any time. However, withdrawing consent may result in our inability to continue providing Site Visitors with access to the Site.

With respect to Site Visitors' personal information, Securly, Inc. and Securly Ltd. are the controllers of Site Visitors' personal information.

We may collect information about Site Visitors, including personal information (as defined by applicable privacy law), directly from Site Visitors, from third parties, or automatically through Site Visitors' use of the Site. We may combine certain information we collect from these various sources.

a. Information We Collect Directly from Site Visitors

We collect information (including personal information) from Site Visitors directly as set out below.

- **Account and Registration Information.** We collect personal information from Site Visitors who sign up for an account with us, including name and email address. We may also ask or allow Site Visitors to submit additional account information, such as phone number, student name, student school, location of school. Site Visitors may browse parts of our Site without creating an account.
- **Communication.** We collect personal information from Site Visitors who communicate with us, including a Site Visitor's name and email address. We may also ask or allow Site Visitors to submit additional account information, such as a phone number. Site Visitors may browse parts of our Site without creating an account.
- **Customer Support.** We collect personal information Site Visitors provide when submitting a request through our Site, such as an email address, or if Site Visitors otherwise contact our customer support services via email, phone, or chat, related to an inquiry or complaint. We keep a copy of such records in our customer files.
- **Newsletters and Updates.** Site Visitors can also sign up to receive emails and offers from us by submitting a name, email address, and zip code or area code. For information on how to opt-out of receiving newsletters and updates via email please see below.
- **Other Information We Collect Regarding Site Visitors' Usage of Our Site.** We collect personal information about your use of our Site, such as your purchase history, online related activity such as sites visited, online searches and videos watched, email content, email address, and geolocation information.

b. Information We Collect from Third-Party Sources

We may also collect information about Site Visitors from third parties, which we combine with the information we have collected via the Site.

Information We Collect Automatically

We automatically collect information about Site Visitors through the use of our Site, including Site Visitors' IP addresses ("Usage Data"). For more information, please see the Cookie and Other Tracking Mechanisms Section further below.

c. Purposes and Legal Bases of Use for Processing Site Visitor Information

We process Site Visitors' personal information for the following legal bases:

Performance of Contract: We process Site Visitors' personal information as necessary to enter into or carry out the performance of a contract with you, for example creating your customer account and processing your payments, or with a school or other institutional customer.

Our Legitimate Business Interests. We process Site Visitors' personal information in furtherance of our legitimate business interests, which are not overridden by Site Visitors' interests and fundamental rights, including:

- Performance of contracts with customers and other parties
- Implementation and operation of support services for our business operations
- Improving our Site and services, developing reports, and similar purposes
- Customer relationship management and improving our Site and services, including other forms of marketing and analytics
- Fraud detection and prevention, including misuse of our Site or services
- Physical, IT, and network perimeter security
- Internal investigations
- Mergers, acquisitions, and reorganization, and other business transactions, including related negotiations

Compliance with Laws. We process Site Visitors' personal information to comply with our legal obligations, including those in the area of labor and employment law, social security, and data protection, tax, and other corporate compliance laws, and/or to defend against legal claims.

With Your Consent: We process Site Visitors' personal information where we have Site Visitors' consent. For example, for some forms of direct marketing, or for the setting of certain cookies, the GDPR, where it applies, and other applicable laws give Site Visitors the right to withdraw consent, which Site Visitors can do at any time by contacting us using the details set out at the end of this Policy.

Vital Interest. In addition, in rare cases we may process Site Visitors' personal information where necessary to protect the vital interests of any individual.

d. How We Use Site Visitor Information

Providing and Improving Services. To maintain and improve our services; to develop new features, products, or services; to perform technical operations, such as updating software; to authenticate a Site Visitor as a valid user; to prevent fraudulent activity on our platform; and for other customer service purposes.

Responding to requests. To respond to Site Visitors' inquiries, fulfill orders and requests.

Personalizing Content and Ads. We may use the information we collect about Site Visitors to personalize the information and content we display to Site Visitors, including to tailor the content

and information that we may send or display to Site Visitors, and to otherwise personalize Site Visitors' experiences, including providing more relevant ads.

Marketing and Communications. We may use information about Site Visitors to send product or service updates; to respond to inquiries; to provide news, special offers, promotions, and other information we think may interest Site Visitors; and for other informational, marketing, or promotional purposes. Our communications with Site Visitors may include communications via email. Site Visitors may opt-out of such communications at all times by following the opt-out instructions contained in the e-mail. Please note that it may take up to 10 business days for us to process opt-out requests. If Site Visitors opt-out of receiving emails about recommendations or other information, but subscribe to our services, we may still send Site Visitors transactional e-mails, such as about any account or services the Site Visitor has requested or received from us. *We do not use personal information of Students or children for any marketing purpose.*

Research and Analytics. We may use information about Site Visitors to analyze how Site Visitors interact with our Site; to monitor and analyze usage and activity trends; and for other research, analytical, and statistical purposes.

Protecting Our Legal Rights and Preventing Misuse. We may use information about Site Visitors to protect the Site and our business operations; to prevent and detect fraud, unauthorized activities and access, and other misuse; where we believe necessary to investigate, prevent or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety or legal rights of any person or third party, or violations of our Terms of Use or this Policy.

Complying with Legal Obligations. We may use information about Site Visitors to comply with the law or legal proceedings. For example, we may disclose information in response to subpoenas, court order, and other lawful requests by regulators and law enforcement, including responding to national security or law enforcement disclosure requirements.

General Business Operations. We may use information about Site Visitors to consider and implement mergers, acquisitions, reorganizations, and other business transactions, and, where necessary, to administer our general business, accounting, recordkeeping, and legal functions.

Aggregate, De-identified or Anonymous Data. We may also use information about Site Visitors to create and use aggregate, anonymous and de-identified data to assess, improve and develop our business, products, and services, and for similar research and analytics purposes. This information is not generally subject to the restrictions in this Policy, provided it does not identify and could not be used to identify a particular individual.

e. How We Disclose Site Visitor Information

In general, we disclose Site Visitors' personal information we collect as follows:

Affiliates. We may share Site Visitors' personal information with our affiliates, whose handling of personal information is subject to this Policy.

Service Providers. We may disclose the information we collect from Site Visitors' to our third-party vendors, service providers, marketing partners, third parties, contractors or agents who perform functions on our behalf so we can provide you with the Site. These may include companies that send emails to our customers and prospective customers; help us track email response rates, views, and forwards; provide advertisements about products of interest to Site Visitors; and collect data about how Site Visitors, customers, and prospective customers interact with our products over time.

Business Transfers. We may disclose Site Visitor information to another entity in connection with an acquisition or merger, sale or transfer of our assets, bankruptcy proceeding or as part of any other similar business transfer, including during negotiations related to such transactions.

In Response to Legal Process. We also may disclose the information we collect from Site Visitors in order to comply with the law, a judicial proceeding, court order, or other legal process, such as in response to a court order or a subpoena.

To Protect Us and Others. We also may disclose the information we collect from Site Visitors where we believe it is necessary to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety of any person, violations of our Terms of Use or this Policy, or as evidence in litigation in which we are involved.

Aggregate and De-Identified Information. We may share aggregate or otherwise de-identified information about Site Visitors with third parties for marketing, advertising, research, or similar purposes.

f. Use of Cookies and Other Tracking Mechanisms on the Securly Site

We and our third-party service providers may use cookies, log files, Web beacons and other tracking mechanisms to track information about your use of our Site. These technologies are not used on our Services. We may combine this information with other personal information we collect from Site Visitors (and our third-party service providers may do so on our behalf).

Cookies. Cookies are alphanumeric identifiers that we transfer to a Site Visitor's computer's hard drive through the web browser for record-keeping purposes. Some cookies allow us to make it easier for Site Visitors to navigate our Site, while others are used to enable a faster login process or to allow us to track Site Visitors' activities on our Site. There are two types of cookies: session and persistent cookies.

Disabling Cookies. Most web browsers automatically accept cookies, but if you prefer, Site Visitors can edit browser options to block them in the future. The Help portion of the toolbar on most browsers will tell you how to prevent your computer from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. Site Visitors who disable cookies will be able to browse certain areas of the Site, but some features may not function. Please keep in mind that without cookies Site Visitors may not have access to certain features on this Site, including certain personalized content.

Clear GIFs, Pixel Tags and Other Technologies. Clear GIFs are tiny graphics with a unique identifier, similar in function to cookies. In contrast to cookies, which are stored on a Site Visitor's computer's hard drive, clear GIFs are embedded invisibly on web pages. We may use clear GIFs (a.k.a. web beacons, web bugs or pixel tags) in connection with our Site to, among other things, track the activities of Site Visitors, help us manage content, and compile statistics about Site usage. We and our third-party service providers may also use clear GIFs in HTML e-mails to you, to help us track e-mail response rates, identify when our e-mails are viewed, and track whether our e-mails are forwarded.

Third Party Analytics. We use automated devices and applications, such as Google Analytics, to evaluate usage of our Site. We also may use other analytic means to evaluate our Site. We use these tools to help us improve our Site, performance, and Site Visitors' experience. These entities may use cookies and other tracking technologies to perform their services.

Geolocation Information. We may use geolocation information related to Site Visitors for the purpose of administering our Site.

Do-Not-Track Signals. Our Site does not currently respond to do-not-track signals. For more information about do-not-track signals, please click [here](#). Site Visitors may, however, disable certain tracking as discussed in the Cookies and Other Tracking Mechanisms section above (e.g., by disabling cookies).

g. Interest-Based Advertising for Site Visitors

We may work with third parties such as network advertisers to assist us in displaying advertisements on third-party websites, and to evaluate the success of our advertising

campaigns. We may use information about Site Visitors for these purposes.

Site Visitors may opt-out of many third-party ad networks, including those operated by members of the Network Advertising Initiative (“NAI”) and the Digital Advertising Alliance (“DAA”). For more information regarding this practice by NAI members and DAA members, and choices regarding information used by these companies, including how to opt out of ad networks operated by NAI and DAA members, please visit their respective websites:

Canada: <http://youradchoices.ca>

EU: <http://youonlinechoices.eu>

US: <http://aboutads.info>; <https://optout.networkadvertising.org/>

Opting out of participation in the ad networks does not opt Site Visitors out of being served advertising. Site Visitors may continue to receive generic or “contextual” ads on our Site, for example, based on the particular website that you are viewing (i.e., contextual advertising). Site Visitors may also continue to receive targeted ads on other websites, from companies that do not participate in the above programs. Please note that opt-out mechanisms are cookie based; so, if Site Visitors delete cookies, configure browsers to block or reject cookies, or use another device, the opt-out will no longer be effective.

h. Security of Site Visitor Personal Information

The security of Site Visitors’ personal information is important to us. We have implemented a security program designed to protect the information we collect through our Site from loss, misuse, unauthorized access, disclosure, alteration, and destruction. However, given the nature of information security, there is no guarantee that our Site will be 100% secure.

We encourage Site Visitors to help protect the security of personal information. For instance, Site Visitors should never give out personal credentials when using the Site. Furthermore, Site Visitor are responsible for maintaining the security of any personal computing device using the Site. We are not responsible for any lost, stolen, or compromised passwords or for any activity on Site Visitor accounts via unauthorized password activity.

i. International Transfers

Securly, Inc. is headquartered in the United States of America and has operations and service providers in the United States and other jurisdictions. As such, we and our service providers may transfer your personal information to, or access it in, jurisdictions (including the United States, India, and Mexico) that may not provide levels of data protection equivalent to your home jurisdiction. We will take steps to ensure that your personal information receives an adequate

level of protection in the jurisdictions in which we process it in accordance with applicable laws, including through appropriate written data processing terms and/or data transfer agreements.

If you are in the European Economic Area (“EEA”) or the United Kingdom (“UK”), and we process your personal information in a jurisdiction that the relevant regulator has deemed to not provide an adequate level of data protection (a “third country”), we rely upon legal measures to adequately protect your personal information. These measures include standard contractual clauses approved by the European Commission or another method approved by the European Commission as providing adequate safeguards for the protection of personal information when transferred to a third country. You have a right to obtain details of the mechanism under which your personal information is transferred outside of the EEA; you may request such details by contacting us as set forth in the “Contact us” section below.

j. No Automated Decision-Making

Securly itself does not take any actions that affect the legal rights of persons; Securly is a tool that helps Parents, Schools, and others make better informed decisions about how to protect and guide the children in their care. Our services do not make automated decisions that have legal impacts on anyone without human review. Although our services may block a particular person from a particular site at a particular moment, the information from the services and the decision to continue to block any particular sites are always subject to human review.

k. Data Subject Rights

If you live in the EEA or other jurisdictions, including Australia, California, Canada, the United Kingdom, and certain other jurisdictions, you may have certain data subject rights. These rights vary, but they may include the following:

- **Right of access:** You can ask us to: confirm whether we are processing your personal information; give you a copy of that information; provide you with other information about your personal information such as what data we have, what we use it for, who we disclose it to, whether we transfer it abroad and how we protect it, how long we keep it for, what rights you have, how you can make a complaint, where we got your information from and whether we have carried out any profiling, to the extent that such information has not already been provided to you in this Policy.
- **Right to rectify and complete personal information:** You can ask us to rectify inaccurate information. We may seek to verify the accuracy of the data before rectifying it.
- **Right of erasure:** You can ask us to erase your personal information, but only where: it is no longer needed for the purposes for which it was collected; you have withdrawn your consent (where the data processing was based on consent); following a successful right to object (see

'Objection' below); it has been processed unlawfully; or to comply with a legal obligation to which we are subject. We are not required to comply with your request to erase your personal information if the processing of your personal information is necessary: for compliance with a legal obligation; or for the establishment, exercise or defense of legal claims. There are certain other circumstances in which we are not required to comply with your erasure request, although these two are the most likely circumstances in which we would deny that request.

- Right of restriction: You can ask us to restrict (i.e., keep but not use) your personal information, but only where: its accuracy is contested, to allow us to verify its accuracy; the processing is unlawful, but you do not want it erased; it is no longer needed for the purposes for which it was collected, but we still need it to establish, exercise or defend legal claims; you have exercised the right to object, and verification of overriding grounds is pending. We can continue to use your personal information following a request for restriction, where: we have your consent; to establish, exercise or defend legal claims; or to protect the rights of another natural or legal person.
- Right to object to our use of your personal information for direct marketing purposes: You can request that we change the manner in which we contact you for marketing purposes. You can request that we not transfer your personal information to unaffiliated third parties for the purposes of direct marketing or any other purposes.
- Right to object for other purposes: You have the right to object at any time to any processing of your personal information which has our legitimate interests as its legal basis. You may exercise this right without incurring any costs. If you raise an objection, we have an opportunity to demonstrate that we have compelling legitimate interests which override your rights and freedoms. The right to object does not exist, in particular, if the processing of your personal information is necessary to take steps prior to entering into a contract or to perform a contract already concluded.
- Right to (data) portability: You can ask us to provide your personal information to you in a structured, commonly used, machine-readable format, or you can ask to have it 'ported' directly to another Data Controller, but only where our processing is based on your consent and the processing is carried out by automated means.
- Right to withdraw consent: You can withdraw your consent in respect of any processing of personal information which is based upon a consent which you have previously provided.
- Right to obtain a copy of safeguards: you can ask to obtain a copy of, or reference to, the safeguards under which your personal information is transferred outside the EU/EEA. We may redact data transfer agreements to protect commercial terms.
- Right to lodge a complaint with your local supervisory authority: You have a right to lodge a complaint with your local supervisory authority if you have concerns about how we are processing your personal information. We ask that you please attempt to resolve any issue with us first, although you have a right to contact your supervisory authority at any time.

You can make a request to exercise these rights by contacting us at support@securly.com or calling 1 (855) 732-8759 (ext. 101). We will review your request and respond accordingly. The rights described herein are not absolute.

You will not have to pay a fee for the disclosure of your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for disclosure is manifestly unfounded or excessive. We will not provide disclosure of your personal data more than twice in any 12-month period.

Individuals who submit requests for access or erasure of personal information will be required to verify their identity by answering certain questions. We will not disclose or delete any information until such individual's identity is verified.

You may designate an authorized agent to submit a request on your behalf by providing that agent with your written permission. If an agent makes a request on your behalf, we may still ask that you verify your identity directly with us before we can honor the request.

Agents who make requests on behalf of individuals will be required to verify the request by submitting written authorization from the individual. We will not honor any requests from agents until authorization is verified.

We do not sell personal information, and we will not discriminate on the basis that you have exercised any of your rights under the California Consumer Privacy Act.

I. Retention

We will generally keep Site Visitors' personal information only for as long as it remains necessary for the identified purposes for which it was collected or as authorized or required by law. We may retain certain data as necessary to prevent fraud or future abuse, or for legitimate business purposes, such as analysis of aggregated data, account recovery, or if required by law.

We will retain Students' and Educators' data as directed by Schools for their purposes.

All retained personal information will remain subject to the terms of this Policy.

m. Changes to this Policy

This Policy is current as of the date set forth above. We may change this Policy from time to time, so please be sure to check back periodically. We will post any changes to this Policy on our [Site](#). If we make any changes to this Policy that materially affect our practices with regard to

personal information, we will endeavor to provide you with notice in advance of such change by prominently highlighting the change on our Site or make other appropriate notice to you.

n. Links

When you visit our Site and leave to go to another linked site, we are not responsible for the content or availability of the linked site. Please be advised that if you enter into a transaction on the third-party site, we do not represent either the third party or you. Further, the privacy and security policies of the linked site may differ from ours.

o. Shine the Light

Under California Civil Code Section 1798.83, Californians are entitled to request information relating to whether a business has disclosed personal information to any third parties for the third parties' direct marketing purposes. Californians who wish to request further information about our compliance with this statute or who have questions, more generally, about our Privacy Policy and our privacy commitments and our Site should contact us as set out in the "Contact Us" section above.

p. Contact Us

If you have any questions, comments, or concerns about the privacy aspects of our Site or services or would like to make a complaint, please contact:

David Hinkle
Vice President of Engineering US/Acting CSO
Securly, Inc.
5600 77 Center Drive,
Suite 350 Charlotte, NC
United States
support@securly.com
1 (855) 732-8759 (ext. 101)

University Laboratory School Software Addendum

Part One: Data Security Addendum

Vendor/Operator (referred to as Vendor or Operator) acknowledges and agrees that compliance with this Addendum in its entirety for the term of the contract and any renewals is a material requirement and condition of this contract. If the Parties determine that any clause in this section is not applicable to this contract it may be stricken without affecting the remaining subsections.

UNLESS SPECIFICALLY EXEMPTED, THE FOLLOWING CONFIDENTIALITY AND DATA SECURITY REQUIREMENTS APPLY TO ALL DATA MADE AVAILABLE TO THE VENDOR UNDER THE TERMS OF THIS AGREEMENT.

REQUIRED CONDITIONS:

1. **Order of Precedence:**

- a. To the extent, any provision in this Addendum is inconsistent or incompatible to terms included elsewhere in this Agreement, the parties agree that this Addendum shall take precedence and the conflicting provisions shall be null and void.

2. **Definitions:** The following terms shall be defined as follows for purposes of the Agreement.

- i. The term **SOPPA Covered Information** means personally identifiable information or material or information that is linked to personally identifiable information or material in any media or format that is not publicly available and is any of the following:
 1. Created by or provided to an Operator by a student or the student's parent or legal guardian in the course of the student's, parent's, or legal guardian's use of the Operator's site, service, or application for K through 12 school purposes.
 2. Created by or provided to an Operator by an employee or agent of a school or school district for K through 12 school purposes.
 3. Gathered by an Operator through the operation of its site, service, or application for K through 12 school purposes and personally identifies a student, including, but not limited to, information in the student's educational record or electronic mail, first and last name, home address, telephone number, electronic mail address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, a social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information.
- ii. The term **Personally Identifiable & Protected University Data** shall include an individual's name first or last, e-mail address or password in an unencrypted or redact form when used in combination one or more of the following data elements including: an (i) identification numbers (e.g. individual's government-issued identification number or social security number, driver's license number); (ii) information protected by federal or state law (e.g. ethnicity, race, religion, disability status, veterans status, etc.), (iii) financial data (including account numbers, credit card number, or other information that would permit access to an individual's financial data; (iii) biometric or health data; or (iv.) other data that if released could create a safety or security concern for the University or members of the University community.
- iii. University Data includes any information provided by the University pursuant to the Agreement.

3. **University Data & SOPPA Covered Information Security Protections:** Vendor shall provide commercially reasonable and adequate protection on its network and systems to protect University Data and SOPPA Covered Information from unauthorized access, acquisition, destruction, use modification or disclosure that shall include but not be limited to include firewalls and intrusion detection/prevention, authentication and encryption capabilities (including mobile devices, USB storage devices and backup media) in accordance with standard industry practices.

- a. **Use of Data:** Vendor agrees that any and all University Data and SOPPA Covered Information exchanged shall be used expressly and solely for the purposes enumerated in the Agreement.
- b. **Data Transmission & Storage:** In general, Vendor shall implement administrative, physical and technical safeguards to protect University Data and SOPPA Covered Information that are no less rigorous than accepted industry practices. Vendor agrees that University Data and SOPPA Covered Information must be stored and transmitted in accordance with standard industry encryption standards. Personally Identifiable & Protected University Data and SOPPA Covered Information may not be processed or stored outside the U.S.

- c. **Third-Party Assurances / Subcontractors:** Vendor may only release University Data and SOPPA Covered Information to a subcontractor, affiliate or other third party with the designated University authorized official's prior written consent and provided that such subcontractor, affiliate, or other third party agrees to comply with all provisions of this Agreement.
- d. **Return/Destruction of Data:**
 - i. As applicable and in accordance with law, within a reasonable time period after termination of this Agreement, for any reason, Vendor shall return or destroy (as specified by the University) all University Data and SOPPA Covered Information and indexing information received from University, or created or received by Vendor on behalf of the University. This provision shall apply to data in the possession of subcontractors or agents of Vendor.
 - ii. Destruction of University Data and SOPPA Covered Information will be conducted in accordance with standard industry practices deemed acceptable by the University and Illinois State Record Act requirements.
 - iii. Vendor shall provide proof or certification of destruction of the data to the University's Information Security Officer.
- e. **Data Processing Integrity:** As applicable, Vendor shall take commercially reasonable measures, including regular data integrity audits, to protect Data against deterioration or degradation of data quality and authenticity. Vendor will maintain appropriate contingency / recovery plans for any University Data and SOPPA Covered Information in the event of loss of data or breach.

4. **Breach:**

- a. **Notice:** Vendor, including any subcontractors, affiliates, and third parties, shall report in the most expedient timeframe possible but no later than 48 hours to the University Information Security Officer (i) any breach of security involving, or potentially involving, University Data and SOPPA Covered Information, or (ii) any use or disclosure of University Data and SOPPA Covered Information other than the Permitted Uses or breach of federal and state privacy laws. Vendor shall fully cooperate with the University with respect thereto. The University Information Security Officer can be contacted e-mailing informationsecurityoffice@illinoisstate.edu.
- b. **Indemnification:** Vendor shall indemnify, defend and hold University harmless from and against all third-party claims, actions, suits and proceedings resulting from the release of any University Data and SOPPA Covered Information, including the University's costs and reasonable attorneys' fees which arise as a result of Vendor's failure to safeguard University Data and SOPPA Covered Information as provided in this Agreement. Any limitations of liability contained in the Agreement shall not be applicable to Vendor's obligations pursuant to this section.

ADDITIONAL DATA SECURITY TERMS & CONDITIONS:

Please check those terms and conditions applicable to this Agreement.

☒ **Vendor Certifications:** Prior to performing services which require access to, transmission of and/or storage of **University Data & SOPPA Covered Information**, Vendor will provide a third party certification of compliance with standard industry practices in a form acceptable to the University Information Security Officer.

☒ **FERPA & State Privacy Protections.** Vendor hereby acknowledge and agrees to comply with the limitations on the use and re-disclosure of **University Data and SOPPA Covered Information** from education records as defined in the Family Educational Rights & Privacy Act ("FERPA") 34 CFR § 99.00 et seq. Vendor agrees to comply with all applicable state privacy protections including but not limited to the Illinois School Student Records Act (105 ILCS 10), the Mental Health and Developmental Disabilities Confidentiality Act (740 ILCS 10), the Identity Protection Act (105 ILCS 85), and the Personal Information Protection Act (815 ILCS 530). Vendor agrees that the Vendor is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the school would otherwise use its own employees and is using University Data and SOPPA Covered Information for an authorized purposes and in furtherance of such legitimate educational interest. Vendor further acknowledge and agrees that it shall maintain the confidentiality, and shall not re-disclose, personally Identifiable Information from education records except as authorized by the University in writing.

☒ **SOPPA.** Vendor agrees to comply with all operator prohibitions and restrictions on the use and re-disclosure of **University Data & SOPPA Covered Information** from education records as outlined in the Illinois Student Online Personal Protection Act, 105 ILCS 85, et seq. These include but are not limited to:

- Vendor may not use University Data & Covered Information to engage in targeted advertising, amass profiles on student or the parents, or sell/rent any student information, or disclose info to any third-party, unless such party maintains all required security procedures and practices.
- As required by SOPPA, Vendor agrees, upon request and within reasonable period of time, to provide a copy of any student's information provided or maintained by the Vendor, as operator. Vendor agrees to correct any factual errors within 90 days of such request.
- Vendor may only use data to improve operability/functionality of operator's site, to ensure legal and regulatory compliance, to take precautions against liability, to respond to judicial process, to protect the safety/integrity of users to the site.
- In the event of a breach of SOPPA Covered Information that is attributable to the Vendor, the Vendor agrees to reimburse and indemnify University for any and all costs and expenses University incurs in investigating and remediating the breach, without regard to any limitation of liability provision including but not limited to costs and expenses associated with:
 - Providing notification to parents of students whose data was compromised;
 - Providing credit monitoring to those students whose data was exposed in a manner that a reasonable person would believe may impact the student's credit or financial security;
 - Legal fees, audit costs, fines, and any other fees or damages imposed against the University as a result of the breach; and
 - Provision of any other notification or fulfilling any other requirements as required by law.

☐ **Health Insurance Portability and Accountability Act ("HIPAA"):** If the Vendor is a "covered entity" as that term is defined under HIPAA, the Vendor shall enter into a Business Associate Agreement with the University. If the Vendor is not a "covered entity" as that term is defined under HIPAA, the Vendor acknowledges i) any students working at the Vendor's site or under the Vendor's supervision and control are part of the Vendor's "workforce" as defined in HIPAA Privacy Regulations at 43 C.F.R. 160.103, and ii) no Business Associate agreement is required between the University and Facility. The Facility will provide the necessary HIPAA training to students and students will be expected to comply with HIPAA and any other confidentiality requirements of the Facility.

☐ **PCI Standards:** If, in the course of providing services to University, Vendor has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, Vendor shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at Service Provider's sole cost and expense.

☐ **Vendor Monitoring/Audit:** With prior written notice, University (or its agent or affiliate) may audit Vendor's use of the University Data to ensure that Vendor is in compliance with the terms of this Agreement. Vendor will keep complete and accurate records of all

use of University data, including a log file of all employees with access to University Data. University may at its own expense and upon no less than five working days written notice audit Vendor's use, access, or maintenance of the University Data. As part of such audit, University is entitled to obtain physical and electronic data concerning use of University's data upon submitting a reasonable request to Vendor. Such audit will not interfere unreasonably with Vendor's business activities, will be conducted no more often than once per calendar year at a location, unless a previous audit disclosed a material breach. If an audit reveals the Vendor has breached this Agreement, University may immediately terminate the Agreement.

Illinois State University reserves the right and the parties agree to amend the Data Security Addendum and related Agreement to address required data security requirement changes in law, including those changes that may apply under the European Union General Data Protection Regulations, effective May 25, 2018.

Part 2: University & Illinois Procurement Code Addendum

The Board of Trustees of Illinois State University (University, ISU), a body corporate and politic of the State of Illinois and the Vendor are entering into a contract/agreement. For the parties' mutual convenience, the parties are using the Vendor's Contract Form. This Addendum is incorporated into the Vendor's Contract Form and made an integral part thereof.

Vendor acknowledges and agrees that the Vendor's Contract Form may include some types of clauses or sales terms not acceptable to the University because of statutory restrictions or other policy considerations. If the Parties determine that any provision of this Addendum in this section is not applicable to this contract it may be stricken without affecting the remaining subsections.

1. Order of Precedence:

- a. To the extent, any provision in this Addendum is inconsistent or incompatible to the Vendor's Contract Form, the parties agree that this Addendum shall take precedence and the conflicting provisions of the Vendor's Contract Form shall be null and void.

2. Insurance:

- a. Illinois State University shall not be required to maintain any type of insurance for the Vendor's benefit.
- b. During all times relevant to this agreement, Vendor shall maintain and keep in effect applicable general liability insurance with limits acceptable to the Board of Trustees of Illinois State University, and shall provide proof of coverage upon request. Additional insurance coverage, as specified in subsection c below, may be required for this agreement depending upon the services provided by the Vendor

3. Confidential Information:

- a. Confidential Information may be made available to the Vendor under this Agreement. The Vendor agrees to i) protect any Confidential Information from unauthorized use or disclosure; ii) disclose Confidential Information only to employees and other representatives who have agreed to comply with this agreement; and iii) use the Confidential Information only for the purposes authorized in this Agreement.
- b. All Confidential Information remains the property of the University.
- c. "Confidential Information" means any information provided by the University whether of a technical, business or other nature that is disclosed to the Vendor that is designated as Confidential by the University, that is protected from disclosure by applicable state or federal law, or that the Vendor has reason to believe is confidential, proprietary, or trade secret information of the University. Confidential Information does not include any information that: (a) was acquired lawfully by the Vendor or independently developed or acquired by the Vendor outside this Agreement; (b) is or becomes part of the public domain through no fault of the Vendor; or, (c) is authorized for release by written notice from University to Vendor; or (d) is otherwise required to be disclosed by law.
- d. ISU reserves the right to disclose contract purchase information as required by the State of Illinois Freedom of Information Act without pre-notification or approval from the Vendor.

4. Governing Law:

- a. Notwithstanding any provision to the contrary, the Vendor's Contract Form shall be governed and construed in accordance with the laws of the State of Illinois.
- b. For venue purposes, it is deemed that all obligations of the parties created hereunder are performed in McLean County, Illinois.

5. Term:

- a. Notwithstanding any provision, the term of the contract (including original and renewal terms) shall not exceed 10 years in total.
- b. No term will automatically renew regardless of stated required notification periods. All renewals will only be valid with the issuance of a University purchase order or other written direction from University.

6. **Indemnification/Hold Harmless/Limitation of Liability:**

- a. It is understood and agreed that neither party to this agreement shall be liable for any negligent or wrongful acts, either of commission or omission, chargeable to the other, unless such liability is imposed by law, and that this agreement shall not be construed as seeking to either enlarge or diminish any obligation or duty owed by one party against the other or against a third party.
- b. The University shall not agree to any additional provision:
 - i. Requiring the University to indemnify or hold harmless the Vendor for any act or omission.
 - ii. Releasing the Vendor or any other entity or person from its legal liability, or limiting liability, or unlawful or negligent conduct or failure to comply with any duty recognized or imposed by applicable law.
 - iii. Requiring the University to make payments for total or partial compensation or payment for lost profit or liquidated damages if the Agreement is terminated before the end of the term.
 - iv. Limiting the liability of the Vendor for property damage or personal injury.
 - v. Binding the University to any arbitration or to the decision of any arbitration board, commission, panel or other entity.
 - vi. Obligating the University to pay costs of collection or attorney's fees.
 - vii. Granting the Vendor a security of interest in property of Illinois State University.
 - viii. Changing the time period within which claims can be made or actions can be brought under the laws of the State of Illinois.
 - ix. Requiring the University to waive the sovereignty of Illinois, waiver of any right to a jury trial, increasing the University's liability beyond that authorized in the Illinois Tort Claims Act, or authorizing Vendor to execute any settlement obligation that would bind the University without the consent of the Board of Trustees of Illinois State University and/or the Illinois Attorney General, as applicable.

7. **Payment Obligations:**

- a. All amounts, including but not limited to interest and/or late charges, owed by the University under the Vendor's Contract Form shall be made in accordance with applicable provisions of the Illinois Prompt Payment Act.

8. **Independent Contractor:** In Vendor's performance under this Agreement, the Vendor acts and will act as an independent contractor and not as an agent or employee of Illinois State University.

9. **Use of University Name & Facilities:** Vendor shall not use the name of the University in any written material including but not limited to brochures, letters, and circulars, without the prior written consent of University. If

applicable, Vendor's use of University Facilities shall comply with all University policies, procedures and requirements.

10. **Force Majeure Provisions:** It is agreed that no claim for damages, losses or liability may be made by either party upon the occurrence of any circumstance, whether directly or indirectly, beyond the control of either party (including without limitation strikes, work stoppages, accidents, acts of war or terrorism, civil or military disturbances, nuclear or natural catastrophes or acts of God, business interruptions, disease, national or local emergency, government action or inaction, travel restrictions, loss or malfunctions of utilities, communications or computer (software and hardware) services ("a Force Majeure Event")), to the extent that such circumstance delays or otherwise makes it illegal or impossible for a party to satisfy its performance obligations under the Agreement. In the event of a Force Majeure Event, the parties agree to negotiate in good faith any modifications of the terms of this Agreement that may be necessary or appropriate in order to resume performance obligations under the Agreement. However, the contract is subject to termination/cancellation by the non-declaring party, unless the parties mutually agree, in writing, to amend the Agreement. As soon as reasonably practicable after a Force Majeure Event occurs, the non-declaring party will provide a written notice to the other party (or parties) that specifies the Agreement termination date. In the event of a termination due to a Force Majeure Event, the Vendor will refund to University all recoverable expenses and 50% of any documented, reasonable, nonrecoverable expenses incurred by Vendor prior to the date of termination. Vendor agrees to provide University with documentation, acceptable to the University, in its sole discretion, that details reasonable, nonrecoverable expenses retained by Vendor relating to the Force Majeure Event.

11. **Procurement Code Required Certifications:**

- a. Vendor acknowledges and agrees that compliance with the attached Certifications and Additional Terms for the term of the contract and any renewals is a material requirement and condition of this 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.
- b. This subsection, in its entirety, applies to subcontractors used on the 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 University.
- c. If this 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 University by the date specified by the University and in no event later than July 1 of each year that this contract remains in effect.

12. **Compliance:**

- a. **Statutory Compliance:** All commitments by the University under this Agreement are subject to constitutional and statutory limitations and restrictions binding upon the University. Vendor agrees to comply with all applicable federal, state, and local laws, orders and regulations.
- b. **University Policies and Procedures:** Vendor agrees to comply with applicable University policies and procedures, as applicable.

- c. **Nondiscrimination:** Vendor agrees to comply with all applicable federal and state nondiscrimination, equal opportunity and affirmative action laws, orders and regulations. Vendor shall not engage in unlawful discrimination or harassment against any person because of race, color, religion, sex, national origin, ancestry, age, marital status, protective order status, disability, unfavorable discharge from the military, or status as a disabled veteran or a veteran of the Vietnam era in the performance of this agreement.
 - d. **Taxes:** The Agreement shall not obligate the University to pay taxes unless otherwise required by law.
 - e. **Withholding/Legal Status:** Vendor shall provide true and correct information regarding its Federal Tax Payer Identification Number (FEIN), tax withholding status and legal status information. Any change in the Vendor's tax withholding status must be immediately reported to the University by Vendor. If a W-8 or W-9 form is required, payment will not be made prior to receipt of a completed form.
 - f. **Export Control:**
 - i. University agrees to comply with applicable U.S. laws, regulations, orders or other restrictions on exports and further shall not sell, license or re-export, directly, or indirectly, any information, data, products, items subject to the Agreement to any person or entity for sale in any country or territory, if, to the knowledge of University, such action would cause the Vendor to be in violation of any such laws or regulations now or hereafter in effect.
 - ii. Vendor shall also notify the University if any of the individuals, equipment, data, services provided or other commitments made or subject to the Agreement are subject to the U.S. Export Administration Regulations, controlled by the International Traffic in Arms Regulations, subject to Office of Foreign Assets Control restrictions, or otherwise subject to export restrictions by a federal agency.
13. **Assignment:** This contract may not be assigned, in whole or in part, by either party without the prior written approval of the other party, except in connection with a merger or sale of all or substantially all of the assets of such party provided, however, that the obligations of such party under this Contract shall not be extinguished or otherwise affected by any such assignment.

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.

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 therequirements 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.