Appendix A

Compliance With New York State Education Law Section 2-d Addendum ("Addendum")

The parties to the Agreement are the Monroe 1 Board of Cooperative Educational Services ("BOCES") and SECURLY, Inc. ("Vendor"). BOCES is an educational agency, as that term is used in Section 2-d of the New York State Education Law ("Section 2-d") and its implementing regulations, and Vendor is a third party contractor, as that term is used in Section 2-d and its implementing regulations. BOCES and Vendor have entered into the Agreement to conform to the requirements of Section 2-d and its implementing regulations. To the extent that any term of any other agreement or document conflicts with the terms of the Agreement, the terms of the Agreement shall apply and be given effect.

Definitions

As used in the Agreement and related documents, the following terms shall have the following meanings: "Student Data" means personally identifiable information from student records that Vendor receives from an educational agency (including BOCES or a Participating School District) in connection with providing Services under the Agreement.

"Personally Identifiable Information" ("PII") as applied to Student Data, means personally identifiable information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA), at 20 USC 1232g.

"Third Party Contractor," "Contractor" or "Vendor" means any person or entity, other than an educational agency, that receives Student Data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including, but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs.

"BOCES" means Monroe #1 Board of Cooperative Educational Services.

"Parent" means a parent, legal guardian, or person in parental relation to a student.

"Student" means any person attending or seeking to enroll in an educational agency.
"Eligible Student" means a student eighteen years or older.

"State-protected Data" means Student Data, as applicable to Vendor's product/service.

"Participating School District" means a public school district or board of cooperative educational services that obtains access to Vendor's product/service through a cooperative educational services agreement ("CoSer") with BOCES, or other entity that obtains access to Vendor's product/service through an agreement with BOCES, and also includes BOCES when it uses the Vendor's product/service to support its own educational programs or operations.

"Breach" means the unauthorized access, use, or disclosure of personally identifiable information.
"Commercial or marketing purpose" means the sale of PII; and the direct or indirect use or disclosure of State-protected Data to derive a profit, advertise, or develop, improve, or market products or services to students other than as may be expressly authorized by the parties in writing (the "Services").

"Disclose", "Disclosure," and "Release" mean to intentionally or unintentionally permit access to State-protected Data; and to intentionally or unintentionally release, transfer, or otherwise communicate State-protected Data to someone not authorized by contract, consent, or law to receive that State-protected Data.

Vendor Obligations and Agreements

Vendor agrees that it shall comply with the following obligations with respect to any student data received in connection with providing Services under the Agreement and any failure to fulfill one of these statutory or regulatory obligations shall be a breach of the Agreement. Vendor shall:

a. limit internal access to education records only to those employees and subcontractors that are determined to have legitimate educational interests in accessing the data within the meaning

of Section 2-d, its implementing regulations and FERPA (e.g., the individual needs access in order to fulfill his/her responsibilities in providing the contracted services);

b. only use personally identifiable information for the explicit purpose authorized by the Agreement, and must/will not use it for any purpose other than that explicitly authorized in the Agreement or by the parties in writing;

c. not disclose any personally identifiable information received from BOCES or a Participating School District to any other party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under the Agreement, unless (i) if student PII, the Vendor or that other party has obtained the prior written consent of the parent or eligible student, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

d. maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the personally identifiable information in its custody;

e. use encryption technology to protect data while in motion or in its custody (i.e., in rest) from unauthorized disclosure by rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5 using a technology or methodology specified or permitted by the secretary of the U S.);

f. not sell personally identifiable information received from BOCES or a Participating School District nor use or disclose it for any marketing or commercial purpose unless otherwise expressly authorized by the Services, or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;

g. notify the educational agency from which student data is received of any breach of security resulting in an unauthorized release of such data by Vendor or its assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay, in compliance with New York law and regulation;

h. reasonably cooperate with educational agencies and law enforcement to protect the integrity of investigations into any breach or unauthorized release of personally identifiable information by Vendor;

i. adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework, Version 1.1, that are in substantial compliance with the BOCES data security and privacy policy, and that comply with Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth below, as well as all applicable federal, state and local laws, rules and regulations;

j. acknowledge and hereby agrees that the State-protected Data which Vendor receives or has access to pursuant to the Agreement may originate from several Participating School Districts located across New York State. Vendor acknowledges that the State-protected Data belongs to and is owned by the Participating School District or student from which it originates;

k. acknowledge and hereby agrees that if Vendor has an online terms of service and/or Privacy Policy that may be applicable to its customers or users of its product/service, to the extent that any term of such online terms of service or Privacy Policy conflicts with applicable law or regulation, the terms of the applicable law or regulation shall apply;

l. acknowledge and hereby agrees that Vendor shall promptly pay for or reimburse the educational agency for the full third party cost of a legally required breach notification to parents and eligible students due to the unauthorized release of student data caused by Vendor or its agents or assignee;

m. ensure that employees, assignees and agents of Contractor who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access to such data; and

n. ensure that any subcontractor that performs Contractor's obligations pursuant to the Agreement is legally bound by legally compliant data protection obligations imposed on the Contractor by law, the Agreement and the Agreement.

Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security
(https://www.monroe.edu/domain/1478)

The Monroe #1 BOCES seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our operations.

The Monroe #1 BOCES seeks to ensure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the BOCES has posted this Parents' Bill of Rights for Data Privacy and Security.

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record. The procedures for exercising this right can be found in Student Records Policy 6320. (https://www.monroe.edu/6320)
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing, to:

   Chief Privacy Officer
   New York State Education Department
   Room 863 EBA
   89 Washington Avenue
   Albany, New York 12234.

   or
   Monroe One Data Protection Officer
   William Gregory
   Monroe #1 BOCES
   41 O'Connor Road
   Fairport, NY 14450

Supplemental Information About Agreement Between SECURLY and BOCES

(a) The exclusive purposes for which the personally identifiable information provided by BOCES or a Participating School District will be used by Vendor is to provide SECURLY's PASS solution to BOCES or other Participating School District pursuant to a BOCES Purchase Order.

(b) Personally identifiable information received by Vendor, or by any assignee of Vendor, from BOCES or from a Participating School District shall not be sold or used for marketing purposes.

(c) Personally identifiable information received by Vendor, or by any assignee of Vendor shall not be shared with a sub-contractor except pursuant to a written contract that binds such a party to at least the same data protection and security requirements imposed on Vendor under the Agreement, as well as all applicable state and federal laws and regulations.

(d) The effective date of the Agreement shall be 07/21/2024 and the Agreement shall remain in effect until 06/30/2024 unless sooner by either party for any reason upon thirty (30) days' notice.

(e) Upon expiration or termination of the Agreement without a successor or renewal agreement in place, and upon request from BOCES or a Participating School District, Vendor shall transfer all educational agency data to the educational agency in a format agreed upon by the parties. Vendor shall thereafter securely delete all educational agency data remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies) as well as any and all educational agency data maintained on behalf of Vendor in secure data center facilities, other than any data that Vendor is required to maintain pursuant to law, regulation or audit requirements. Vendor shall ensure that no copy, summary or extract of the educational agency data or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the secure data center facilities unless Vendor is required to keep such data for legal, regulator, or audit purposes, in which case the data will be retained in compliance with the terms of the Agreement. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers permanently removed with no possibility of reidentification), they each agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to the BOCES or Participating School District from an appropriate officer that the requirements of this paragraph have been satisfied in full.

(f) State and federal laws require educational agencies to establish processes for a parent or eligible student to challenge the accuracy of their student data. Third party contractors must cooperate with educational agencies in complying with the law. If a parent or eligible student submits a challenge to the accuracy of student data to the student's district of enrollment and the challenge is upheld, Vendor will cooperate with the educational agency to amend such data.

(g) Vendor shall store and maintain PII in electronic format on systems maintained by Vendor in a secure data center facility in the United States in accordance with its Privacy Policy, NIST Cybersecurity Framework, Version 1.1, and the BOCES data security and privacy policy, Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education, and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth above. Encryption technology will be utilized while data is in motion and at rest, as detailed above.

(h) A copy of Vendor's Data Privacy and Security Plan, which vender affirms complies with 8 N.Y.C.R.R. 121.6 is attached hereto as **Attachment 1** and is incorporated herein by reference as if fully set forth herein.

Meghann Carlin _____ 6/26/2024 _____, 2023

Vendor Signature

ATTACHMENT 1 – Security Plan

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third- party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2- d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York State. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Information security and data privacy are part of our company culture. We begin with company core values and a mission that support data privacy and information security and we carry that culture through all aspects of our business including business continuity and our written information security program.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Securly adheres to a written information security program aligned with NIST Standard 800-53, including a full suite of information security policies, an accountable information security team, background screening, ongoing security awareness and training program, asset management policies, access controls, cryptography for data in transit and at rest, and operations, physical, and environmental security standards.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Prior to Employment, Securly performs background screening of new hires including job history, references, and criminal checks (subject to local laws). Securly requires all new employees to sign comprehensive non-disclosure and confidentiality commitments. During Employment, Securly maintains an information security awareness and training program that includes new hire training. Information Security awareness is enhanced through regular communications using company-wide communications, as necessary. The organization maintains records of security awareness training sessions. Access to information assets is removed in a timely manner for users no longer requiring access to perform their job responsibilities.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	All new vendors and third parties must be thoroughly screened and before entering into a business relationship. Prior to entering into service agreements or contracts, Securly must perform a risk assessment over the prospective vendor's ability to abide by applicable policies and procedures related to security.

5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Securly maintains an incident management response plan that is tested on a regular basis. Affected EAs will be promptly notified of any incident involving unauthorized access to or use of student/teacher/admin data.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Securly enables EAs to access their data at any time, and to direct Securly to delete data during the term of the contract or following termination.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Securly's data destruction policy mandates secure deletion of paper documents and media containing EA data, appropriate to the nature of the media.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Securly's information security program and practices are aligned with NIST Standard 800-53.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

ATTACHMENT 1 – NIST CSF TABLE

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Securly management has: • Identified critical assets in the environment and has assessed the associated threats and vulnerabilities; • Established criteria for determining acceptable use of its information assets; • Hosted critical production information assets in Amazon Web Services; and through that console maintains access to a complete and accurate inventory of current assets used to support the production environment.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Securly is committed to the protection of its Information Technology resources, subject to and consistent with applicable legal requirements. Each user is responsible for the appropriate collection, use, protection and disposal of information and assets to protect from unauthorized use.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Securly has established criteria for determining how data sets and information within the environment should be used, handled and protected, based on its content and level of sensitivity to the business and the company's customers. The company has established means of securely storing data according to the classification.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	On an annual basis, or when a significant change occurs in the environment, management assesses the current risk landscape based on all facets of the business. Management considers threats, vulnerabilities, weaknesses, and environmental impacts to Securly to assist in the creation of objectives and goals and the allocation of resources. At least annually, management engages an independent assessor to examine the effectiveness of controls in the environment and understand Securly's state of compliance with internal policies and/or external frameworks.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Results of scans are reviewed by management to prioritize the resolution of identified vulnerabilities against business objectives.
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	Securly has established a program to monitor and ensure service levels and ongoing compliance of existing vendors and third parties. All new vendors and third parties must be thoroughly screened and before entering into a business relationship. Prior to entering into service agreements or contracts, Securly must perform a risk assessment over the prospective vendor's ability to abide by applicable policies and procedures related to security.

Function	Category	Contractor Response
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Any new instance of access within the environment must follow standard procedures for obtaining authorization prior to accessing information assets. Securly requires that users authenticate to networks, operating systems, databases, applications, and tools in the environment using unique IDs and strong passwords in order to access information assets. Access to company information attests is reviewed periodically to ensure ongoing compliance with access policies. Users are reviewed for continued appropriateness of access rights and segregation of duties, and to ensure that access is removed timely for terminated employees or changes in job roles and responsibilities. Access to information assets is removed in a timely manner for users no longer requiring access to perform their job responsibilities. Access to sensitive information and administrative access to systems and tools is restricted to authorized individuals and limited to as few individuals as necessary to perform relevant functions.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	Securly has established procedures to ensure that employees and contractors are informed of their job roles and responsibilities, and up to date on the requirements of current policies.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	All personal data is encrypted in transit and at rest. On an annual basis, or when a significant change occurs in the environment, management assesses the current risk landscape based on all facets of the business. Management considers threats, vulnerabilities, weaknesses, and environmental impacts to Securly to assist in the creation of objectives and goals and the allocation of resources.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	To ensure that significant updates to software are designed and developed according to management's intentions, Securly has established a process to obtain necessary inputs, documentation and approvals for the creation of updates. To ensure that new features are created in accordance with the approved design, management has developed processes to test new changes to functionality, alignment with management's intentions and impact to customers prior to release. Management has implemented a series of required approvals for any changes to the production environment supporting products and services. To ensure that updates and new features are appropriately deployed to the production environment according to management's intentions, Securly has implemented measures to ensure the integrity of the deployment, minimal impact to customers and segregation of duties between the environments.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Securly has established a periodic schedule for patching various layers of systems and infrastructure in the environment. Further patching is performed as needed based on releases from vendors and events in the external environment.

Function	Category	Contractor Response
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Securly has established measures to protect production and supporting environments from malicious software to reduce the risk of disruption of service and loss of data. Endpoint Anti-virus technology is deployed and secured such that users cannot modify or disable protection. Production information systems are audited for internal vulnerability regularly and external vulnerability scans (penetration testing) occurs at least quarterly.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Securly has implemented an entity wide security awareness program to identify weaknesses and vulnerabilities so that security incidents and breaches may be prevented, and detected when they occur.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	On an annual basis, or when a significant change occurs in the environment, management assesses the current risk landscape based on all facets of the business. Management considers threats, vulnerabilities, weaknesses, and environmental impacts to Securly to assist in the creation of objectives and goals and the allocation of resources.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Securly has implemented measures to detect security vulnerabilities in the environment using external tools and authoritative sources. Prioritized components of the environment are scanned periodically to identify vulnerabilities that present a threat to critical information assets. At least annually, management engages an independent assessor to examine the effectiveness of controls in the environment and understand Securly's state of compliance with internal policies and/or external frameworks.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	To ensure continued business operations during and following any critical incidents that results in a disruption to normal operational capabilities, management has developed a plan to address scenarios that may arise from the occurrence of such disruptive events and incidents. The results of the annual test of incident response and disaster recovery policies and procedures are reported to stakeholders and analyzed to make improvements to the existing plan.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Securly has implemented an entity wide security awareness program to identify weaknesses and vulnerabilities so that security incidents and breaches may be prevented, and detected when they occur. Notice of a security incident must be given to affected internal and external parties as required. Such disclosures, along with the time, date and method of disclosure, is documented in the ticket.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Incidents that have been identified and entered into the tracking system, are assigned to the appropriate owners for resolution. Responsible parties document activities associated with the containment, resolution and other recovery efforts associated with the incident.

Function	Category	Contractor Response
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	To ensure that the business continuity and disaster recovery plan is effective for meeting recovery time objectives, management conducts an annual test of the plan. The results of the test are reported to stakeholders and analyzed to make improvements to the existing plan. In the event of an actual live event scenario that requires the plan to be used, no testing is required.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	To ensure that the business continuity and disaster recovery plan is effective for meeting recovery time objectives, management conducts an annual test of the plan. The results of the test are reported to stakeholders and analyzed to make improvements to the existing plan. In the event of an actual live event scenario that requires the plan to be used, no testing is required.
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	To ensure the ongoing availability of critical data, management has established a schedule of backups and data redundancy. Backups and replications are monitored for failures, and resolved in a timely manner
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	To ensure continued business operations during and following any critical incidents that results in a disruption to normal operational capabilities, management has developed a plan to address scenarios that may arise from the occurrence of such disruptive events and incidents. After a major incident has been resolved and appropriate parties notified of the occurrence, a postmortem that includes root cause analysis is performed, along with the documentation of any lessons learned. Policies and procedures are reassessed and updated as needed in the event of a major or pervasive incident.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Notice of the incident must be given to affected internal and external parties as required. Such disclosures, along with the time, date and method of disclosure, is documented in the ticket.

APPENDIX B
SECURLY TERMS AND CONDITIONS OF SERVICE

The Agreement applies to the order form to which these Terms and Conditions of Service are attached (collectively, the "Agreement"). This TOS is made by and between Securly, Inc. ("Company" or "Securly"), a Delaware corporation with offices at 5600 77 Center Drive, Suite 350 Charlotte, NC and its the Monroe One Educational Services ("Customer"). The effective date of the TOS is the effective date of the relevant order is referred to herein as the "Effective Date."

1. Services. Company will provide to Customer the cloud-based software products and services identified in the purchase order (the "Order") that incorporates these terms and conditions (collectively, the "Services" and, each, a "Service"). If there is a conflict or ambiguity between any term of this TOS and the Order, the terms and conditions of the Order shall control. The Services may include, without limitation, Company's cloud-based web filtering, online activity monitoring for cyberbullying, auditing software, mobile device management software, tablet, and other computer asset 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 ("Users").

2. Security. Company represents and covenants that it maintains appropriate administrative, technical and physical security measures to protect Customer data and personal information, including User Data (as defined in Section 4 below), to the extent reasonably necessary for the performance of the Services consistent with all applicable state and federal laws and regulations. In the event of a breach or suspected breach of any privacy or security measures described herein that has become known to Company, Company will immediately notify Customer thereof, and use its commercially reasonable efforts to remedy such breach.

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

4. Ownership

(a) Ownership of the Service; Intellectual Property. Company shall retain all title to and ownership of and all proprietary rights with respect to the Services (including all software used to provide the Services and all portions thereof (including all derivatives or improvements thereof), 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 the 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").

(b) Ownership of User Data. The Services may allow Customer to track and gather a range of data and information regarding its Users ("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).

(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. Company may disclose Customer personal information to its service providers as necessary for Company to provide the services to Customer. 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. Company certifies that it understands and will comply with the restrictions on the processing of Customer personal information as set forth in this Section 4 (a).

(d) Data sources. Customer acknowledges that, dependent 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.

(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. Company hereby grants Customer a non-exclusive, non-sublicensable, and non-transferable license, for the term of the 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 (iTunes 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.

5. Privacy Policy

(a) 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, Children's Privacy Policy and Notice of Privacy Practices (together the "Privacy Policy"), which include 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 Company's collection, use and disclosure of Minor User Data by Company in order to provide the Services to Customer. Customer further acknowledges, and Company agrees to provide, Customer an opportunity to review the Minor User Data, and to request that such data be deleted and/or no longer collected or used (which may impact the availability of the Services). By executing the Agreement, 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.

6. Customer Responsibilities, Warranties and Restrictions

(a) Customer agrees that it shall not 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 expressly stated 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); (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 shall not (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 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.

(d) Customer represents, covenants, and warrants that Customer will use the Services only in compliance with the terms and conditions of the Agreement and all applicable laws and regulations. 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 the 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 the Agreement in accordance with its terms and conditions.

(f) Where Customer's 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 6(f); (iv) it will maintain adequate records of consents and its compliance with this Section 6(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) Where Customer's use of the Services include visitor management, verification and tracking of visitors and other individuals, and related services or applications ("VMS"): Customer represents, warrants and covenants 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) that 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.

(h) There is no applicable law, regulation, rule, or other governmental requirement (A) which in any way restricts or limits the duty of Customer to fully perform and comply with all obligations of Customer as set forth in the Agreement, or (B) which impairs the rights of Company as set forth in the Agreement; and (iii) the software for the Services provided under the Agreement will be treated as "commercial computer software" and "commercial computer software documentation" under any applicable governmental laws, regulations or rules.

(i) 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 the Agreement, pursuant to DFARS §227.7202.

7. 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 the 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) the Discloser's User Data. 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 the Agreement and for a period of five (5) years following the termination or expiration of the 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 the 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 the Agreement. The Recipient shall be responsible for any breach of this Section 7 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 the 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, or upon the termination of the Agreement. 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 7.

(d) Recipient acknowledges that the disclosure of Confidential Information in breach of the terms of this Section 7 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 the Agreement. This provision will not in any way limit such other remedies as may be available to the Discloser, whether under the Agreement, at law, or in equity.

8. Billing and Payment. 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 the 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. 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 the 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 the Agreement.

9. Term and Termination

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

(b) Any and all provisions in the Agreement which would reasonably be expected to be performed after the termination or expiration of the 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.

10. Company Warranties, Company Disclaimers, and Exclusive Remedies

(a) Company warrants to Customer that it will provide the Services in all material respects as described in the applicable end user documentation, if any, and will provide such Services in a professional manner and in accordance with generally accepted industry practices. 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.

(b) 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.

(c) NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THE AGREEMENT, COMPANY DOES NOT GUARANTEE OR WARRANT (A) THAT THE SERVICES WILL COMPLY WITH THE REQUIREMENTS OF THE CHILDREN'S INTERNET PROTECTION ACT, (B) THAT THE SERVICES WILL FUNCTION TO PREVENT MINORS FROM BEING EXPOSED TO INAPPROPRIATE, HARMFUL, UNSAFE, OR OBSCENE CONTENT ONLINE, (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.

(d) 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 COMMERCIALLY 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 COMMERCIALLY REASONABLE EFFORTS TO PROVIDE CUSTOMER WITH REASONABLE OPPORTUNITY TO ACCESS THE SERVICES FOR THE PURPOSES OF SECURING AND BACKING UP CUSTOMER'S USER DATA.

(e) 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.

11. Limitation of Liability. EXCEPT WITH REGARD TO INDEMNIFICATION OBLIGATIONS SET FORTH IN THIS AGREEMENT, BOTH PARTIES EXPRESSLY UNDERSTAND AND AGREE THAT NEITHER PARTY SHALL BE LIABLE TO THE OTHER UNDER THE 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 THE 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 7, AND WITHOUT AFFECTING THE LIMITATIONS OF LIABILITY SET FORTH IN SECTION 10, IN NO EVENT SHALL COMPANY'S AGGREGATE LIABILITY OF ANY TYPE UNDER THE 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.

12. Indemnification. Company shall defend Customer against any Claim made or brought against Customer by a third party 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, on condition that Customer (a) promptly gives Company written notice of the Claim; (b) gives Company sole control of the defense and settlement of the Claim (provided that Company may not settle any Claim unless the settlement unconditionally release Customer of all liability); and (c) provides reasonable assistance in connection with the defense (at Company's reasonable expense). 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 the Agreement upon notice. Company will have no liability under the 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 the Agreement. This Section

12(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.

13. 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.

14. Relationship of the Parties. The parties are independent contractors with respect to each other, and nothing in the 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.

15. Force Majeure. Except payment obligations, any delay in or failure of performance by a party under the Agreement will not be considered a breach of the 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 the Agreement continues for thirty (30) days or more, then the other party may terminate the 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 15 (i.e. wherein Customer does not or otherwise cannot terminate the Agreement pursuant to this Section 15), Customer shall not be entitled to any service credit or refund.

16. Binding Effect; Assignment; Third Parties. The terms and conditions of the Agreement shall be binding on the parties and all successors and permitted assigns of the foregoing. Securly may assign or transfer, by operation of law or otherwise, any or all of its rights, burdens, duties or obligations under the 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 the obligations of Securly 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. Securly will notify the District in writing within sixty (60) days of any such change of control. To the extent the assignee is an entity prohibited from conducting business in the State of New York, Customer will have the option to terminate the Agreement. The 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 the Agreement.

17. Modification; Waiver. All modifications to or waivers of any terms and conditions of the Agreement (including any exhibit) must be in a writing that is signed by the parties hereto and expressly references the Agreement. No waiver of any breach of any provision of the 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.

18. Governing Law. The Agreement and all actions arising out of or in connection with the Agreement shall be construed under and governed by and interpreted in accordance with the laws of the State of New York, without regard to the conflicts of law provisions thereof.

19. Severability. In the event that any provision of the Agreement shall be held invalid, illegal, or unenforceable by a court with jurisdiction over the parties to the 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 the 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 the 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. The 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 the Agreement are for convenience of reference only and have no legal effect.