GARDEN CITY UNION FREE SCHOOL DISTRICT
EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Securly, Inc. (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the GARDEN CITY UNION FREE SCHOOL DISTRICT (the "District") and Contractor to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that the District's Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"Protected Data" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by the District. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of the District as that term is defined in § 99.3 of FERPA,

-AND-

"Personally identifiable information" from the records of the District relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with District policy(ies) on data security and privacy. Contractor shall promptly reimburse the District for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of

Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of the District's data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of the District's Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

3. Specifies how officers or employees of the Contractor and its assignees 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;

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

6. Specifies whether Protected Data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the contract is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);

2. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;

3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of the District's Parent Bill of Rights.

NAME OF PROVIDER: Securly, Inc.

BY: Kaitlin Flynn _____ **DATED:** 05/28/2025

Return to:

Lauren Maguire
Director of Information Technology
Garden City Union Free School District
56 Cathedral Avenue
Garden City, NY 11530
maguirel@gcufsd.net

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

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.

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at https://www.nist.gov/cyberframework/new-framework. Please use additional pages if needed.

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
	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	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	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

Function	Category	Contractor Response
	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.
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
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurityrelated duties and responsibilities consistent with related policies,	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

Function	Category	Contractor Response
	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
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and	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.
	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
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
	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

Function	Category	Contractor Response
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.
	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

Function	Category	Contractor Response
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking	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.