EXHIBIT D

Data Sharing and Confidentiality Agreement

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. **Purpose**

(a) This Exhibit supplements the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES' website.

(b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

(d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of all Protected Data it receives in accordance with applicable federal and state law (including but not limited to Section 2-d) and this DSC Agreement, as may be amended by the Parties, and Erie 1 BOCES' policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy, and that Erie 1 BOCES will provide Vendor with a copy of its policy upon request.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.
https://www.securly.com/privacy
https://www.securly.com/students-privacy

Additional elements of Vendor's Data Security and Privacy Plan are as follows: See Attachment 1 to Exhibit D

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

(b) As required by the NIST Cybersecurity Framework, in order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA,
    a. Vendor will have the following reasonable administrative, technical, operational, and physical safeguards and practices in place throughout the term of the MLSA:
        i. Data Security:
            1. Data-at-rest & data-in-transit is encrypted
            2. Data leak protections are implemented
        ii. Information Protection Processes and Procedures:
            1. Data destruction is performed according to contract and agreements
            2. A plan for vulnerability management is developed and implemented

iii. Protective Technology:
1. Log/audit records are ascertained, implemented, documented, and reviewed according to policy
2. Network communications are protected

iv. Identity Management, Authentication and Access Control:
1. Credentials and identities are issued, verified, managed, audited, and revoked, as applicable, for authorized dev

(c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(e) Vendor ___X___will _____will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:

(i) the parent or eligible student has provided prior written consent; or
(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **<u>Notification of Breach and Unauthorized Release</u>**

(a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).

(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

(e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)

ERIE 1 BOCES

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

(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.

(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 for public review at **http://www.nysed.gov/data-privacy-security/student-data-inventory**, or 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 the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website **http://www.nysed.gov/data-privacy-security/report-improper-disclosure**.

BY THE VENDOR:

DocuSigned by:
Michaelann Carlin
8514C05B02104FA...

Signature

Michaelann Carlin

Printed Name

Director of Revenue Operations

Title

9/4/2024

Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND SECURLY, INC.

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with Securly, Inc. which governs the availability to Participating Educational Agencies of the following Product(s):

Securly Pass Core & Pass Premium

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with Securly, Inc. which governs the availability to Participating Educational Agencies of the following Product(s):

Securly Pass Core & Securly Pass Premium

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by:

a. All new vendors and third parties are thoroughly screened and before entering into a business relationship.

b. Prior to entering into service agreements or contracts, Securly performs a risk assessment of the prospective vendor's ability to abide by applicable policies and procedures related to security.

c. Securly contractually prohibits service providers from using or disclosing Customer Information for any purpose other than providing the contracted for services and obligates them to protect such data under terms and conditions that meet or exceed the requirements of our customer contracts.

Duration of MLSA and Protected Data Upon Expiration:

The MLSA commences on July 1, 2024 and expires on June 30, 2027.
Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.

Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

Attachment 1 to Exhibit D
Securly, Inc. Data Privacy and Security Plan

Attachment 1 to Exhibit D - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

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 D-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.

Function	Category	Contractor Response
	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.
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

Function	Category	Contractor Response
		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.
	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.

Function	Category	Contractor Response
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.
	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

Function	Category	Contractor Response
		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.