STANDARD STUDENT DATA PRIVACY AGREEMENT

WA-NDPA Standard

Version 1.0

Local Education Agency (LEA):

Enumclaw School District

and

Provider:

Securly, Inc.

DATE:

3/23/23

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between:

School District: Enumclaw School District, located at: 2929 McDougall Ave. Enumclaw, WA 98022 ("**LEA**") and

Provider: Securly, Inc., located at: 5600 77 Center Drive, Suite 350 Charlotte, North Carolina, USA (the "**Provider**").

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions.** ***Check if Required.***
   - ☑ If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.
   - ☑ If checked, LEA and Provider agree to the additional terms of modifications set forth in **Exhibit "H"**
   - ☑ If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. [Reserved]

5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**").

6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: _____ Title: _____

Address: 5600 77 Center Drive, Suite 350 Charlotte, North Carolina, USA

Phone: _____ Email: _____

The designated representative for the LEA for this DPA is:

Name: Jill Burnes Title: Deputy Superintendent

Address: 2929 McDougall Ave. Enumclaw, WA 98022

Phone: 360-802-7124 Email: jill_burnes@enumclaw.wed

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

LEA:

By: Jill Burnes Date: 3/23/23

Printed Name: Jill Burnes Title/Position: Deputy Superintendent

Name of Provider: Securly, Inc.

By: Michaelann Carlin Date: 3/23/23

Printed Name: Michaelann Carlin Title/Position: Director of Revenue Operations

STANDARD CLAUSES
Version 3.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data.

2. **Student Data to Be Provided**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.

3. **DPA Definitions**. The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.

2. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct, as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the

Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA. [See Modification at Exhibit "G"]
3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on

behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D.

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits. [See modification at Exhibit "G"]

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with

the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security**. The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

4. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

(1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

i. The name and contact information of the reporting LEA subject to this section.
ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

(3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable

information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

(5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination**. In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.

2. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.

3. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit H, the SDPC Standard Clauses, and/or the Supplemental State Terms, Exhibit H will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement**. This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

6. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

7. **Successors Bound**: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

9. **Waiver**. No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"

DESCRIPTION OF SERVICES

Unless specied otherwise, this DPA covers access to and use of Securly, Inc.'s existing Site, Software and Services, as well as any future Sites, Software or Services provided by Securly, Inc. including, without limitation, all subdomains, software and mobile applications, and products owned and operated by Securly, Inc., its subsidiaries and/or other affiliates.

Filter- Cloud-based content filter solution that keeps school districts CIPA compliant. Filter works on any school owned device, regardless of location to prevent students from accessing harmful or pornographic material.

Classroom- A tool that allows teachers to manage student devices during class to ensure students are engaged and on task.

Aware- Student safety and wellness tool that scans email, docs, images, searches, sites, and social media for signs of bullying, self harm, and violence. If Aware detects an issue, it alerts the designated school personnel.

On-call- Securly's team of student safety analysts who monitor data 24/7. If the data indicates a student is at risk of hurting themselves or others, our team will contact the designee from the school district.

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	✓
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	✓
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	✓
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	✓
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	✓
Parent/Guardian Name	First and/or Last	✓
Schedule	Student scheduled courses	✓

Category of Data	Elements	Check if Used by Your System
	Teacher names	✓
Special Indicator	English language learner information	
	Low-income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	✓
	Phone	
Student Identifiers	Local (School district) ID number	✓
	State ID number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	✓
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Students pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	

Category of Data	Elements	Check if Used by Your System
Other	Please list each additional data element used, stored, or collected by your application:	☐
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	☐

EXHIBIT "C"

DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records,

videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

District or LEA: to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

☐ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

Categories of data:

☐ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

☐ Disposition shall be by destruction or deletion of data.

☐ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

Special instructions:

3. Schedule of Disposition

Data shall be disposed of by the following date:

☐ As soon as commercially practicable.

☐ By Date:

4. Signature

_____ _____

Authorized Representative of LEA Date

5. Verification of Disposition of Data

_____ _____

Authorized Representative of Company Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Enumclaw School District ("Originating LEA") which is dated 3/23/23, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material changes in the applicable privacy statues; (2) a material changes in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address: michael@securly.com.

Name of Provider: Securly, Inc.

BY: Michaelann Carlin Date: 3/23/23

Printed Name: Michaelann Carlin Title/Position: Director of Revenue Operations

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between originating LEA: and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

Name of Subscribing LEA:

By: _____ Date: _____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____

Title: _____

Address: _____

Telephone Number: _____

Email: _____

EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

2/24/2020

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

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
☐	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
☐	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
☐	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
☐	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
☐	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
☐	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

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

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

EXHIBIT "G" – Supplemental SDPC State Terms for [State]
Version 1.0

1. Recitals shall have the following sections added: This Amendment for SDPC State Terms for Washington ("**Amendment**") is entered into on the date of full execution (the "**Effective Date**") and is incorporated into and made a part of the Student Data Privacy Agreement ("**DPA**") by and between:

School District: Enumclaw School District, located at: 2929 McDougall Ave. Enumclaw, WA 98022 (the "**LEA**") and
Provider Name: Securly, Inc., located at: 5600 77 Center Drive, Suite 350 Charlotte, North Carolina, USA (the "**Provider**").

All capitalized terms not otherwise defined herein shall have the meaning set forth in the DPA.

WHEREAS, the Provider is providing educational or digital services to LEA, which services include: (a) cloud-based services for the digital storage, management, and retrieval of pupil records; and/or (b) digital educational software that authorizes Provider to access, store, and use pupil records; and

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 C.F.R. Part 99); the Protection of Pupil Rights Amendment ("**PPRA**") at 20 U.S.C. §1232h; and the Children's Online Privacy Protection Act ("**COPPA**") at 15 U.S.C. § 6501-6506 (16 C.F.R. Part 312), accordingly, the Provider and LEA have executed the DPA, which establishes their respective obligations and duties in order to comply with such applicable laws;

WHEREAS, the Provider will provide the services to LEA within the State of Washington and the Parties recognizes the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable Washington laws and regulations, such as the Student User Privacy in Education Rights 28.A.604 et seq. and RCW 42.56.590; and other applicable state privacy laws and regulations; and

WHEREAS, the Provider and LEA desire to enter into this Amendment for the purpose of clarifying their respective obligations and duties in order to comply with applicable Washington state laws and regulations.

NOW, THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. **Term**. The term of this Amendment shall expire on the same date as the DPA.

2. **Modification to Article IV, Section 2 of the DPA**. Article 4, Section 2 of the DPA is hereby amended to read as follows:

Authorized Use: The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit "A" or stated in the Service Agreement, or authorized under the statutes referred to herein by this DPA. Provider may use or disclose data to:

(a) Protect the security or integrity of its website, mobile application or online service.

(b) Ensure legal or regulatory compliance or to take precautions against liability.

(c) Respond to or participate in the judicial process.

(d) Protect the safety of users or others on the website, mobile application or online service.

(e) Investigate a matter related to public safety.

In undertaking the activities specified in subsections (a) through (e) above, Provider shall adhere to all applicable data protections contained in this DPA, as well as Federal and Washington State law.

3. **Modification to Article IV, Section 7 of the DPA**, Article IV, section 7 is hereby amended to add the following language:

(iv) providing recommendations for school, educational, or employment purposes within a school service without the response being determined in whole or in part or other consideration from a third party.

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

LEA:

By: Jill Burnes Date: 3.23.23

Printed Name: Jill Burnes Title/Position: Deputy Superintendent

Provider: Securly, Inc.

By: Michaelann Carlin Date: 3/23/23

Printed Name: Michaelann Carlin Title/Position: Director of Revenue Operations

EXHIBIT "H" – Additional Terms or Modifications

Version 1.0

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

This is a free text field that the parties can use to add or modify terms in or to the DPA. If there are no additional or modified terms, this field should read "None."

618-1/4715859.1

830-1/6107877.1

ARTICLE III: DUTIES OF LEA

1. ADD: "In particular, but without limitation, LEA is responsible for providing notice and securing the consent of parents/guardians to Securly processing of such data where such notice and consent is required by applicable law."

ARTICLE IV: DUTIES OF PROVIDER

1. ADD: "LEA agrees to provide copies of or cites for local rules or regulations pertaining to Student Data."

ARTICLE VII: MISCELLANEOUS

1. ADD "and such breach (i) remains uncured within 10 days of receipt of written notice of breach or (ii) cannot be cured."

7. AMMEND last sentence to "The LEA has the authority to terminate the DPA if it demonstrates in writing that the successor to whom the Provider is selling, merging, or otherwise disposing of its business is unable to fulfill Provider's obligations hereunder."

Modifications to Exhibit "F" - Data Security Requirements

Securly's Information Security Management process is aligned with the principles and objections of best industry practices including, e.g., ISO 27001. Our information security policies and procedures are designed to deliver on the following objectives:

- Confidentiality: Only authorized persons have the right to access information.
- Integrity: Only authorized persons can change the information.
- Availability: The information must be accessible to authorized persons whenever it is needed.
- Accountability: Those who have access to information are responsible for ensuring the security of that data and accountable for noncompliance.

Please see the following attached documentation regarding Securly's information security management system:

1. Securly's description of its MDM Student Safety Suite System
2. Securly's Compliance and Security FAQs
3. Securly's SOC2 Audit for 2021, prepared by the independent firm of Moss Adams LLP

I. Securly's Description of Its MDM Student Safety Suite System

A. Services Provided

Securly was founded in 2013 with a single intention: to keep kids safe online. The business is headquartered out of San Jose, California with offices is Charlotte, North Carolina, operations in Cancun, Mexico, and research and development in Pune, India. Securly develops solutions that keep kids safe and engaged online, at school, and at home. From tools that help adults create a kid-friendlier Internet, to an artificial intelligence that recognizes signs of bullying and even intuits risks of self-harm, Securly breaks new ground and innovates to meet modern problems head-on. For every child that we empower to stand strong, for each kid that chooses hope over hopelessness, Securly is motivated to continue forging ahead.

Securly products provide cloud-based web filtering and parental controls that works across schools and homes. Securly products prevent bullying and self-harm by generating alerts for the parents and have a service that monitors 24x7 any suspicious flags raised by the Filter and Auditor.

Securly's Student Safety Suite System represents the scope of this SOC 2 report and is comprised of:

- Filter
- Auditor
- Tipline
- Securly 24

Other solutions offered by Securly that are considered outside the scope of this report include:

- Parent Portal
- School MDM
- Chrome Tools
- PNP Hub

B. Principal Service Commitments and System Requirements

Securly designed its processes and procedures to meet its objectives for its compliance services. Those objectives are based on the service commitments that Securly makes to user entities, the law and regulations that govern the provision of its compliance services, and the financial, operational, and compliance requirements that Securly has established for the services. Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreement.

Security commitments are standardized and include, but are not limited to, the following:

- Host the production cloud infrastructure within multiple Availability Zones and Regions on Amazon Web Services (AWS)
- Encrypt the data at rest, which is stored in Elastic Cloud
- Maintain commercially reasonable administrative, technical, organizational, and physical measures to protect the security of customer data against anticipated threats or hazards
- Maintain servers in good working order with access restricted to qualified employees
- Retain the audit logs and make available as applicable
- Perform annual and quarterly vulnerability assessment and penetration testing on the application and infrastructure
- Have Securly's employees complete online information security training on annual basis
- Require third parties with access to confidential information to sign an agreement with Securly that includes requirements related to confidential information
- Maintain monitoring controls which notify Securly in case any security breaches happen to the infrastructure
- Delete all customer data within 60 days after termination

Securly establishes operational requirements that support the achievement of security commitments and other requirements. Such requirements are communicated in Securly's system policies and procedures, system design documentation, and contracts with customers. Information security polices define an organization-wide approach to how systems and data are protected.

C. Components of the System Used to Provide the Services

1. Infrastructure

AMAZON WEB SERVICES

The Platform-as-a-Service (PaaS) environments that support Securly's production environment in US East (Northern Virginia, Ohio, Northern California, and Oregon), Asia Pacific (Sydney), Canada (Central), and Europe (Ireland and London) are physically located in data centers owned and operated by AWS. AWS manages and is responsible for its own internal processes as related to the logical security of the infrastructure used by Securly. Securly also relies upon AWS for physical access controls, protection of equipment from environmental hazards, and power. Amazon Elastic Compute Cloud (EC2) is used to run and support certain elements of its application infrastructure such as filtering, cyber bulling detection, DNS service, and proxy service on the EC2 instances. Access to the services running in this infrastructure is limited through the use of Access Controls Lists (ACLs) on the security groups associated with the EC2 instances. Customer sensitive data is stored on Elasticsearch and Redis, which is maintained in AWS.

ELASTIC CLOUD

Elastic Cloud is a distributed, real-time search and analytics engine and datastore. Elasticsearch maintains all types of data, including textual, numerical, geospatial, structured, and unstructured. Securly uses Elastic Cloud to store data such as searches performed by the students on Google or Facebook. All data is encrypted at rest by Elastic Cloud.

Securly has an Elastic Cloud cluster deployed in Asia Pacific (Sydney), E.U. (Ireland), U.S. East (Northern Virginia), and US West (Oregon), with platinum support available 24x7x365. Securly has enabled the backup and recovery of Elastic Cloud to recover from any disaster.

FILES.COM

Files.com, previously known as BrickFTP, is a file sharing service used by Securly for customer file upload. Securly creates a unique username and the customer sets the password and uploads the required file. Securly receives notification once the file has been uploaded, and the uploaded data is then imported into the Securly databases.

In addition, other primary infrastructure used to provide Securly's Software-as-a-Service (SaaS) system includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Web Servers	EC2	Deploy the services that are offered to customers
Application Load Balancer	ALB, ELB, NLB	Load-balancing of EC2 clusters and services
Object Storage	S3	Storing certificates, logs, scripts, etc.
DNS Web Service	Route 53	Register Securly domain and subdomain
Relational Database	RDS MySQL Database	Relational database to maintain the customer data
IAM Console	AWS Identity Access Management	Control the access to production environment
Web Application Firewall	AWS WAF	Prevent an attack to the Securly cluster from distributed denial of service (DDoS) attacks
Auto-Scaling	AWS Auto Scaling Groups	Scale the server in peak time
Firewall	Security Groups, NACL	Firewall to ensure security of EC2 and subnets
Compliance Scanning	AWS Config	Compliance scanning of identity and access management (IAM) resources
Security Alerting	AWS GuardDuty	Alerting if any critical malicious activity is detected in the infrastructure

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Logging & Monitoring	CloudWatch, CloudTrail	Logging CPU, memory utilization, and as an alerting engine in case of any emergency
Serverless Computing	Lambda	Execute application features and process
Email Notification	SES, SNS	Notification service to alert in case of any emergency situation
NoSQL Database	Elasticsearch	Store the activity of the students
Code Deployment	CodeDeploy	Configuration management tool and to deploy the code in production environment.
Cache	Elastic Cache	Host Redis so that frequently required data can be accessed immediate.
Certificate Management	Certificate Manager	Manage the SSL certificates of Securly.

2. Software

Securly's Student Safety Suite System represents the scope of this SOC 2 report and is comprised of:

- Filter
- Auditor
- Tipline
- Securly 24

FILTER

Filter is Securly's cloud-based web filtering service for schools that can filter all types of devices, whether they are school-managed or personal devices. Filter provides school administrators with features like custom policy creation, choice of more than 15 categories of content to allow or block, custom blacklists and whitelists, alerts on self-harm or bullying-related activity, and seamless Google, Azure, and Active Directory authentication using G Suite or Office 365. There are three types of Filter deployments that customers can choose from according to type of device and preference:

- *DNS Filter* – Deployment of Filter by configuring the school networks DNS servers to point to Securly Internet Protocol (IP) addresses
- *Smartpac Filter* – Deployment of Filter by installing Proxy auto configurations URL profiles on devices
- *Chrome Extension* – Deployment of Filter by installing Securly's Chrome-based browser extension

AUDITOR

Auditor is Securly's artificial intelligence engine, which typically monitors the activity on Google Drive, Gmail, and Google Docs. It scans all the activity that students are doing on these channels and flags for self-harm and bullying. Alerts detected by this engine are notified to IT Administrators at the given school, delegated administrators, principals, counselors, and parents. Important alerts are handled by Securly's 24.

TIPLINE

Tipline is a Securly solution that helps students and staff members to anonymously report any bullying or violent incidents. It is an easy-to-use method of sharing information about such incidents and every alert is seen and heard by Securly. The reporter can send a tip via the Tipline application, email, text, telephone, or web form.

SECURLY 24

Securly 24 is Securly's dedicated internal incident response team, which works 24x7 and has access to the Filter and Auditor service data. Securly 24 includes one director and seven to eight Security staff (FTE employees in the United States and in a wholly owned subsidiary in India, one FTE in the United Kingdom via a wholly owned subsidiary, and two to three contractors in Mexico). Securly 24 tracks the activities and responds to detected emergencies.

In addition to the Student Safety Suite System, Securly uses the following software systems:

Primary Software	
Software	**Purpose**
Apache Server	Used to host Securly's website
CMS	Used as content management software to build websites
Confluence	Used for maintaining Securly's documents
ElasticCloud	Used to store the student activities that they perform online
Elasticsearch	Used to store the online activities performed by student
Files.com	Used as an FTP server by which customer can share the file to upload parent and student relationship
Firebase	Used for managing mobile app push notifications
Fluentd	Used for shipping user logs to the Elasticsearch database and for triggering AWS lambda events
GitHub	Used as a Code Repository Management
Google	Used for G Suite system and services
G Suite	Used as email, documentation, and maintaining organizational units (OUs)
IPvsdm	Used for IP forwarding
Jenkins	Used by DevOps for automation build deployment and infrastructure creation
JIRA	Used for internal communication and managing the releases, requirements, and tasks
Maxmind	Used for getting IP databases for different geographical regions, which helps to know content on websites based on user geographical location
Monit	Used to monitor the services running on cluster and give PagerDuty alerts
MySQL	Used to store the customer relational data

Primary Software	
Software	**Purpose**
Nagios Logger	Used for monitoring application logs
OpenVPN	Used to provide VPN services to employees
Redis	Used as cache to access the customer data
RingCentral	Used as internal/external conferencing and meeting tool
Rsyslogng	Used for pushing application logs to centralize syslog server
Salesforce	Used for customer support management
Sendy	Used for sending marketing campaign emails
Slack	Used for live discussion as an internal messenger
Splunk	Used to store the student activities that they perform online
Squid Proxy	Used as a proxy to filter the traffic of students activity online
Stack-Driver	Used as a monitoring tool
Unbound	Used as DNS routing to route the traffic to Squid Proxy
VividCortex	Used as a database monitoring tool
Zendesk	Used as a support ticketing tool

3. People

A Board of Directors is in place and oversees management activities. Reporting to the Board of Directors, the Chief Executive Officer and the Chief Revenue Officer are responsible for the overall operation of Securly. The Board of Directors meets quarterly and is consulted and involved in all significant business decisions.

Reporting to the Chief Executive Officer and the Chief Revenue Officer, each member of the senior management team has a distinct, separate responsibility within the organization. Roles and responsibilities have been segregated to the extent possible and a formal organization chart has been developed.

Securly's senior management report directly to the Chief Executive Officer and is listed below:

- Chief Design Officer
- Senior Vice President of Customer Success
- Senior Vice President of Engineering – India
- Senior Vice President of Finance
- Senior Vice President of Sales Operations
- Senior Vice President of Sales
- Senior Vice President of Customer Success
- Vice President of Support
- General Manager of CLT Operations
- General Manager of Classroom and MDM

Securly, Inc. currently has a staff of approximately 160 employees. Roles and responsibilities have been segregated to the extent possible and a formal organization chart has been developed, containing the following main departments (alphabetical order):

- Engineering
- G&A (Finance, HR, etc.)
- Marketing
- Sales
- Support

SENIOR LEADERSHIP TEAM

Overseen by Chief Executive Officer, the Senior Leadership team is responsible for overseeing company-wide activities, establishing, accomplishing goals, marketing, public, analyst relations, account management, engineering implementations, customer support, forging key strategic partnerships, managing the recruiting, hiring, human resources operations of the company, sales, managing the fiscal and day to day operations of the company.

ENGINEERING

Engineering is responsible for developing, testing, deploying, maintaining, and securing software and infrastructure for Securly production applications. These responsibilities are shared among the multiple global teams within Engineering. The teams and their responsibilities are as follows:

- *Software Development* – Responsible for developing the software for the Securly applications, as well as making improvements and enhancements to it per the business needs.
- *Quality Assurance* – Responsible for testing new software, reporting issues with new software, and tracking them to resolution.
- *Project Management* – Responsible for tracking and managing planned infrastructure and software projects, ensuring projects meet deadlines and objectives.

- *DevOps* – Responsible for the build and release of new software, managing the security of Securly's production applications and infrastructure, making changes to production servers, infrastructure, and configurations, ensuring overall availability and reliability of the system, and granting and revoking logical access to systems within Securly production network and infrastructure.
- *Data Team* – Responsible for analyzing data and providing data to internal teams for marketing, decision-making, and engineering projects.

SUPPORT

Support is responsible for providing support services to the customers and employees. Support consists of customer support, 24 student safety support, and the IT team.

- *Customer Support* – Responsible for providing technical support to customers through a cloud-based ticketing system and communicating information to customers regarding new issues and/or developments.
- *24 Student Safety Support* – Responsible for alerting schools and 911 about suspicious student activity related to self-harm or bullying.
- *IT Support* – Responsible for managing corporate computing devices, business applications, logical access to internal communication applications and email, supporting toolsets, and employee and contractor identities.
- *Product Management* – Responsible for building features and products for customers, as well as actively communicating the changes to external and internal stakeholders such as customers and employees.
- *Human Resources* – Responsible for onboarding new personnel, defining the role/position of new hires, performing background checks, and administering physical access to Securly corporate offices, and facilitating the employee termination process.

EXTERNAL USERS

The following are the external users that are given access to the system based on their assigned roles and responsibilities at a given school.

- *IT Administrator* – A dedicated IT Administrator can login to the Admin Portal and can access all the features to view the student activities, get the alerts about suspicious behavior of student, and apply the filter policy.
- *Delegated Administrator* – Created by an IT Administrator, a Delegated Administrator is a user that can be any staff member of a school given limited access to the Admin Portal to monitor the student activities within a school.
- *Parents* – Parents can login to the Parent Portal to view their children's activities at school or at home. Parents can also apply settings for what their children can view online.

4. Data

INFORMATION ASSET

Critical production information assets are hosted by AWS. Through the management console, Securly has access to a complete and accurate inventory of current assets used to support the production environment.

DATABASES

Three databases are in use by Securly. These include:

- *Elasticsearch* – Contains all student data. All student online data is logged to Elasticsearch.
- *MySQL* – Infrastructure defers from one cluster to another (moving to EC2 to RDS). Stores all student and school-related data.
- *Redis* – Used as cache for performance and access, containing the data needed to make a filtering decision.

DATA STORAGE

The company has established means of securely storing data according to the classification.

- Restricted and Confidential data is stored using AES 256-bit encryption when stored on any media type.
- Access to cryptographic keys is restricted.
- Public information can be stored on any company computer.
- Hard copies of Restricted or Confidential information must be secured in a locked drawer or file cabinet.
- All Personal Identification Information (PII) is stored on Elasticsearch.
- All associated data device and associated users' device locations and parent student relations is stored in MySQL and Redis.

DATA COMPLIANCE

Securly maintains compliance with the Family Educational Rights and Privacy Act (FERPA).

DATA CLASSIFIED

Securly has established criteria for determining how data sets and information within the environment should be used, handled, and protected, based on their content and level of sensitivity to the business and the company's customers.

Management has identified the following data types:

- *Restricted* – Highly sensitive data that if compromised could put the company at financial or legal risk, may be subject to state/federal/international privacy regulations, Personally Identifiable Information (PII), Personal Health Information (PHI), credit card information, intellectual property (IP), and Social Security Numbers (SSNs)
- *Confidential* – Sensitive data that if compromised would negatively affect the operations or reputation of the company (performance reviews, vendor contracts, trade secrets)
- *Private* – Data that should only be disclosed to employees and authorized vendors and third parties of the company, not appropriate for public disclosure (organizational charts, employee contact information, sales strategy, employee handbooks)
- *Public* – Data that may be freely disclosed to the public (approved marketing materials, contact information, product pricing details)

DATA TRANSMISSION

The company has established means of securely transmitting data according to the classification using cryptography and other security protocols.

- The company uses transport layer security protocols for web and email communications.
- Restricted information cannot be shared over open public wireless networks.

DATA RETENTION

Securly has established a schedule to retain data according to legal and regulatory mandates and to meet the company's SLAs and commitments. Personal data is kept no longer than necessary for the purposes for which it is being processed.

- Information must be stored for at least one year from the date of collection.
- The data and records retention schedule is reviewed annually for ongoing compliance.
- Exceptions to the retention policy must be requested by the relevant business unit and approved by management.

DATA DISPOSAL

Securly has established a schedule to dispose of data according to legal and regulatory mandates, and to meet the company's service level agreements and commitments. Customer Service and Support teams will notify the DevOps team of a customer request to terminate their service. Restricted and Confidential customer data is permanently deleted within 60 days of the customer request.

5. Processes and Procedures

Securly has documented policies and procedures to support the development, operations, maintenance, and monitoring of controls over its physical and logical environments. The policies and procedures are in place so that the systems remain secure and available, information is kept confidential and private, and the integrity of processing is upheld. Specific relevant policies include the following:

INFORMATION SECURITY POLICY

This suite of policies and procedures addresses various components of information security that have been developed to protect Securly's critical assets, data, staff, and customers. Employees are required to acknowledge that they understand and will adhere to the policies. Key topics addressed by the policy include:

- Acceptable Use Policy
- Use and Protection of Mobile Devices
- Physical Security
- Employee Communication and Training
- Anti-Virus and Anti-Malware
- Intrusion Detection System
- Penetration Testing

SOFTWARE DEVELOPMENT LIFECYCLE POLICY

This suite of policies and procedures shows how Securly manages the design, development, testing, and deployment of software. Key topics addressed by the policy include:

- Design and Development
- Testing
- Approvals
- Deployment
- Emergency Procedures

THIRD-PARTY AND VENDOR MANAGEMENT POLICY

This document is intended to assist management and process owners in performing and monitoring activities pertaining to the management of risk associated with the use of vendors and third parties. Key topics addressed by the policy include:

- New Vendor Setup
- Service Level Agreements
- Third-Party Risk Management

DATA CLASSIFICATION AND HANDLING POLICY

This document is intended to assist management and process owners in performing and monitoring activities pertaining to the classification and handling of data and information in order to meet the company's system requirements and service commitments.

Key topics addressed by the policy include:

- Information Assets
- Data Storage
- Classification of Data Types
- Data Transmission
- Data Retention
- Data Disposal

ACCESS AND AUTHENTICATION POLICY

This document is intended to assist management and process owners in performing and monitoring activities performed to manage the risk associated with unauthorized access to information. Key topics addressed by the policy include:

- New or Modified Access
- Authentication
- User Access Review
- Deprovisioning

- Administrative and Privilege Access
- Shared and Generic Accounts

BUSINESS CONTINUITY AND DISASTER RECOVERY POLICY

This document is intended to assist management and process owners in performing and monitoring activities pertaining to the disaster recovery plans and business continuity program in order to meet the company's system requirements and service commitments. Key topics addressed by the policy include:

- Backups, Restoration, and Availability of Data
- Business Continuity Planning
- Annual Testing

INCIDENT MANAGEMENT AND RESPONSE POLICY

This document is intended to assist management and process owners in performing and monitoring activities pertaining to the identification and resolution of security incidents. Key topics addressed by the policy include:

- Incident Monitoring and Identification
- Incident Tracking and Classification
- Containment, Eradication, and Recovery
- Root Cause Analysis

INFORMATION RISK MANAGEMENT POLICY

This document is intended to assist management and process owners in performing and monitoring activities pertaining to the management of risks associated with the company's ability to meet system requirements and service commitments. Key topics addressed by the policy include:

- Internal Risk Assessment
- External Risk and Control Assessment
- Other Information Risk Management Activities

PATCHING AND VULNERABILITY MANAGEMENT POLICY

This document is intended to assist management and process owners in performing and monitoring activities pertaining to the management of security vulnerabilities in order to meet the company's system requirements and service commitments.

Key topics addressed by the policy include:

- Patching
- Vulnerability Scanning
- Reporting, Prioritizing, and Remediation
- Penetration Testing

D. Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

1. Control Environment

MANAGEMENT CONTROL

Securly has established appropriate lines of reporting, which facilitate the flow of information to appropriate people in a timely manner. Roles and responsibilities are segregated based on functional requirements. Securly has an organization chart that defines the organizational structure and reporting lines. Responsibility for the design, development, implementation, maintenance, and monitoring of Securly's security policies has been assigned to the DevOps team. They perform routine updates as technology, industry, regulatory, and business requirements change. The ultimate responsibility of the overall information security is the responsibility of the Chief Executive Officer and the Director of Operations.

A third party performs a background check on all new employees and contractors. This includes an employment check, criminal records check, county records check, SSN trace, and national criminal and sex offender check.

Access to the new employee is requested through an access request form that is approved by the employee's manager.

Management performs the review of subservice organizations by reviewing their SOC 2 reports, and any exceptions noted are addressed. This includes for AWS, Elastic Cloud, and Google.

Any change to the production environment is approved by management, and DevOps is the only one who can make modification to production environment.

SECURITY MANAGEMENT

The Securly security process is described in the Information Security Policy, which consists of following:

- Acceptable Use Policy
- Use and Protection of Mobile Devices
- Physical Security
- Employee Communication and Training
- Anti-Virus and Anti-Malware
- Intrusion Detection System
- Penetration Testing

Securly keeps customer information confidential and data up-to-date and error-free. Securly also keeps systems well-managed, replete with operating system updates, security patches, and with limited access to licensed customers, authorized employees, and contractors.

As a part of security efforts, Securly uses several strategies to detect issues such as:

- Logging user access to any activity on AWS accounts.
- Tracking any modification to the security group with public access.
- Logging work performed on production servers using CloudTrail.
- Tracking vulnerabilities and updates related to the server's operating system and applications.
- Tracking uptime related to the SLAs or other services to the customers.
- Maintaining the Security Charter where quarterly goals for the Security team have been identified and aligned to the roadmap.

In addition, Securly conducts internal web application assessment and penetration testing of production infrastructure and web applications allowing the opportunity to detect more complex security issues within products.

SECURITY POLICIES

Securly has designed several policies to protect the security of the systems, the privacy of customer data, and internal confidential information related to the ability to calculate applicable plans and rates for quotes and proposals. These security policies include:

- *Information Security Policy* – Records policies and procedures for how Securly plans to implement high level information security protections within the organization, including definitions, procedures, and responsibilities.
- *Patching and Vulnerability Management Policy* – Records policies and procedures for how Securly plans to prevent, identify, classify, and accordingly handle vulnerabilities to information assets in the environment.
- *Information Risk Management Policy* – Records policies and procedures for how Securly plans to develop, manage, and control vendor and third-party contracts, relationships, and performance.
- *Incident Management & Response Policy* – Records policies and procedures for how Securly plans to detect and respond to events in the environment that could impact the security of the system and the company's ability to meet its system requirements and service commitments.
- *Access & Authentication Policy* – Records policies and procedures for how Securly plans to manage and control access to information assets to minimize the risk of inappropriate access to data resulting in data loss.
- *Data Classification and Handling Policy* – Records policies and procedures for how Securly plans to identify, classify, and accordingly handle information assets (data) within the environment.

CHANGE MANAGEMENT

Securly uses a Change Management and Software Development Policy to direct change management practices.

DESIGN AND DEVELOPMENT

Securly has established a process to obtain necessary inputs, documentation, and approvals for the creation of updates. The design and development process includes:

- The design and details of all changes to the software must be documented, proposed, and signed off prior to initiating development processes.
- Change specifications are documented to record necessary information including critical issues, system impairments, customer impacts, etc.
- Once the design approval is documented, the responsible Developer creates the new features in their own test environment.

TESTING

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. The testing process includes:

- A risk analysis is performed by the team overseeing the creation of a change or new feature (Developer, Quality Assurance, and Project Manager).
- All changes and new features are tested by a Quality Assurance tester who provides approval that the update has completed testing.
- Quality Assurance testing is performed in a separate environment that is similar to the production environment.
- An impact analysis is performed and documented upon completion of testing.

APPROVALS

Management has implemented a series of required approvals for any changes to the production environment, supporting products, and services. The approvals process includes:

- In addition to design and quality assurance approvals, deployment approvals are required by relevant stakeholders and recorded in the ticketing system prior to deployment.
- If the change is owned and managed by the DevOps team, additional deployment approval is required by the DevOps manager.
- No further changes to the release are permitted after approval.

DEPLOYMENT

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. The deployment process includes:

- Upon receipt of deployment approvals, the change is passed to the Build and Release team within the DevOps team. Access to deploy to production is restricted to members of the Build and Release team, who do not perform development activities.
- Releases are initially deployed to the beta environment, where impact is limited to a small number of customers.
- The Build and Release team monitors the success of the Beta deployment. If no risks or issues are identified, the team continues to deploy the update on a cluster-by-cluster basis, starting with the least populated clusters.

EMERGENCY PROCEDURES

To ensure that processes are in place to quickly respond to customer or internal incidents that require updates to product code or other production environments, management has established procedures for alternative change controls when individuals or teams are not immediately available for timely response. The emergency procedures include:

- In the event of an unplanned event, typically triggered by system impairment, unexpected events from code deployment, or customer-facing downtime, a Priority 0 ticket is created to track the resolution of the issue.
- If the issue is known to be customer-facing, customers on the affected clusters are notified that they are going into safe mode, which limits their functionality, but prevents downtime while triaging and resolving issues.
- Stakeholders are alerted to the identified issue and the DevOps team gets on a call to triage the issue and create a solution.
- Based on the issue, the team rolls back any necessary deployed code.
- Updates and/or fixes are developed and sent directly to Quality Assurance for testing. Quality Assurance specifically tests for implementation of the needed fix. The updates/fixes are deployed to production once Quality Assurance testing is complete.
- A root cause analysis is performed and documentation regarding the details of the change and its necessary approvals is captured within 48 hours of deployment.

DATA BACKUP AND RECOVERY

Securly ensures that the services and operations of Securly can be restored within a defined timeframe in the case of any disaster.

Securly has defined the backup and recovery test plan, which consists of taking backup and testing their restoration annually. Customer and production data is backed up on a nightly basis for MySQL and Redis databases, while Elasticsearch data is backed up on a weekly basis.

Recovery procedures are documented and available to support restores as needed, and the procedures are tested annually.

2. Risk Assessment Process

Leadership and management have implemented a process for identifying, analyzing, and addressing relevant risks and aligning them with the annually developed organizational strategy and objectives.

Securly's risk assessment process identifies and manages risks that could potentially affect Securly's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility.

Securly identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

Securly has established an independent organizational business unit that is responsible for identifying risks to the Securly and monitoring the operation of the company's internal controls. The approach is intended to align Securly's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Securly attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

RISK ANALYSIS

Risk analysis is an essential process to Securly's success. It includes identification of key business processes where potential exposures of some consequence exist, as well as significant changes to those processes. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring, and identification of the control activities necessary to mitigate the risk. Management has identified these control activities and documented them in the Trust Services Category, Criteria, and Related Controls section below. Additionally, management reviews the assessed risk levels on an annual basis and documents the risk assessment in the annual risk program.

POTENTIAL FOR FRAUD

Management considers the potential for fraud when assessing the risks to the company's objectives. The potential for fraud can occur in both financial and non-financial reporting. Other types of fraud include the misappropriation of assets and illegal acts such as violations of governmental laws. Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. Therefore, documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process. Additionally, the risk assessment that is performed on an annual basis, considers the potential for fraud.

RISK MITIGATION

Policies and procedures are in place to guide personnel in risk mitigation activities, including monitoring processes and development of policies, procedures, and communications to meet Securly's objectives during response, mitigation, and recovery efforts. Security stakeholders perform a risk assessment on an annual basis that includes an evaluation of risk mitigation control activities for risks arising from potential business disruptions. Disaster recovery and business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. The plans are reviewed, updated, and approved annually based on the business impact analysis during the annual risk assessment process. The organization obtains insurance to offset financial impact of a risk materializing.

A Third Party and Vendor Management Policy is in place that addresses the following:

- Specific requirements for a vendor and business partner
- Due diligence process prior to accepting new vendors or business partners
- Monitoring process to review vendor and business partner compliance on a periodic basis
- Exception handling
- Termination of contract

PROPRIETARY AND CONFIDENTIAL

All policies are reviewed and updated as needed during the annual risk assessment process.

Vendors are evaluated in accordance with the vendor screening process and approved by management prior to processing customer data. Signed nondisclosure agreements of confidentiality and protection are required before sharing information designated as confidential with third parties. The Senior Leadership team reviews vendor audit reports on at least an annual basis to ensure that third-party providers are in compliance with the organization's requirements.

INTEGRATION WITH RISK ASSESSMENT

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently.

Securly assigns owners to each risk identified during the annual risk assessments, and those owners are responsible for selecting and developing the control activities to mitigate those risks.

3. Information and Communication Systems

Information and communication are integral parts of Securly's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time necessary to conduct, manage, and control Securly's operations.

INTERNAL COMMUNICATION

Securly has implemented various methods of communication to ensure significant events are communicated internally in a timely manner. These methods include company meetings, information sessions, and the use of electronic mail messages to communicate time-sensitive information and Slack-channels to have internal communication.

Securly uses below software for internal communication:

- *JIRA* – Ticketing tool used to track and assign ownership of activities by the DevOps and Engineering teams. JIRA is also used to create support tickets for issues escalated by customers through the Customer Support team and allows for management to monitor and track progress of projects.
- *Slack* – For any live discussion and as internal messenger employee uses Slack.
- *Email* – All important communication happens over email.

EXTERNAL COMMUNICATION

All external communications are handled via Salesforce and Zendesk, and the responsibility for such commitments reside with the Sales/Customer Success team for Salesforce and the Support team of Securly for Zendesk. The Customer Success team uses email to communicate with customers, while the Sales team uses Salesforce, phone calls, and email to communicate with customers.

4. Monitoring Controls

Monitoring of internal controls is a critical aspect in evaluating whether controls are operating as intended and whether they are appropriately modified to reflect the changes in the control environment. Management is responsible for monitoring the quality of internal control performance as a routine part of their activities. Quarterly Security team meetings take place where critical issues are identified and corrective actions are discussed and prioritized based on risk. Additionally, Securly performs internal assessments of their security and availability controls.

The services provided by AWS, Elastic Cloud, Slack, and Atlassian are monitored on a regular basis as part of the day-to-day operations. As they become available, Securly personnel receive and review documentation (SOC reports and/or security certifications) provided by these organizations to help ensure security practices are being followed.

The following are monitoring tools used by Securly:

- *AWS CloudTrail and AWS Config* – Securly has configured an alerting notification in case of any modification to access controls, and uses AWS CloudTrail and AWS Config maintain compliance of access controls and other AWS services.
- *AWS GuardDuty* – Securly uses AWS GuardDuty as a security incident monitoring tool to continuously analyze the DNS and VPC logs. Any malicious incident is notified to Securly's Security team via email notification.
- *CloudWatch* – Securly uses CloudWatch to monitor the CPU and memory utilization of the EC2 instances. It is also used to alert the DevOps team of any suspicious activity if resources become unavailable.

- *Monit* – Monit is the service used by Securly to get PagerDuty alerts if any of the services running on the EC2 instances go down.
- *VividCortex* – Securly uses VividCortex for database monitoring, which typically includes the query running time and database deadlock. VividCortex also helps in monitoring which query runs the most.

E. Trust Services Criteria and Related Controls

Although the applicable trust services criteria, related controls, and management responses to deviations, if any, are presented in Section IV of this report titled "Trust Services Category, Criteria, Related Controls, and Tests of Controls", they are an integral part of Securly's system description throughout the period January 1, 2021 to December 31, 2021.

F. Complementary User Entity Controls

Securly's MDM Student Safety Suite System was designed under the assumption that certain controls would be implemented by the user entities for whom it provides its MDM Student Safety Suite System. In these situations, the application of specific controls at these customer organizations is necessary to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

This section describes additional controls that should be in operation at the customer organizations to complement the controls at Securly. User auditors should consider whether the following controls have been placed in operation by the customers.

Each customer must evaluate its own internal control structure to determine if the identified customer controls are in place. Users are responsible for:

Complementary User Entity Controls	
1	Understanding and complying with their contractual obligations to Securly.
2	Provisioning and removing access to their Securly instances in a secure manner.
3	Ensuring that only authorized users have access to their Securly instances.
4	Notifying Securly in the event of a suspected or known security issue or breach
5	Maintaining their own systems of record.
6	Allowing only authorized personnel to know and understand the services, network, and supporting infrastructure of Securly.
7	Developing their own disaster recovery and business continuity plans which addresses the inability to access or utilize Securly's services.


MOSSADAMS

Securly Compliance & Information Security FAQs:

Last updated: Sep 30, 2022 by Brandon Pav

Ques 1: What Information Securly collects from Customer?

We may collect information, including personal information (as defined by applicable privacy law), directly from you, from third parties such as your child's school, or automatically though your use of the Services. We may combine certain information we collect from these various sources

Information We Collect Directly from You. We collect information (including personal information) from you directly as set out below.

Account and Registration Information. We collect personal information from you when you sign up for an account with us, including your name and email address. We may also ask or allow you to submit additional account information, such as your phone number, student name, student school, location of school. You may browse parts of our Site without creating an account, however, if you would like to use Securly's Services, we ask you to create an account.

Customer Support. We collect personal information you provide, when you submit a request through our Site, such as your email address, or if you otherwise contact our customer support services via email, phone, or chat, related to your enquiry or complaint. We keep a copy of such records in our customer files.

Newsletters and Updates. You can also sign up to receive emails and offers from us by submitting your name, email address, and zip code or area code. For information on how to opt-out of receiving newsletters and updates via email please see below.

Securly Hub. If you purchase our Hub, we collect your name and shipping information and collect certain transactional information related to your purchase. We use third party payment processors who handle our payments. If you decide to connect your Plug 'n Play devices through our Securly Home App, we collect personal information from your connected Hub devices, such as your IP address, Mac Address]. Please note that you are not required to connect your Hub with our Services. However, if you do not connect such device we may not be able to offer you our full range or all of our Services.

Other Information We Collect Regarding Your Usage of Our Services. We collect personal information about your use of our Services, such as your purchase history, online related activity such as sites visited, online searches and videos watched, email content, email address, and geolocation information.

Information We Collect from Third-Party Sources We may also collect information about you from third parties, which we append to the information we have collected. Information

We Collect Automatically. We automatically collect information about you through your use of our Services, including log files, IP address, app identifier, advertising ID, location info, browser type, device type, domain name, the website that led you to our Services, the website to which you go after leaving our Services, the dates and times you access our Services, and the links you

click and your other activities within the Services ("**Usage Data**"). If you authorize us to collect your geolocation information, we will collect it while our App is running on your device. You can disable our access to your location services by changing your device's location settings. For more information please see the Cookie and Other Tracking Mechanisms Section further below.

Ques 2: How we use customer information?

Providing and Improving Services. To provide you with, maintain, and improve our Services; to develop new features, products, or services; to perform technical operations, such as updating software; to authenticate you as a valid user; to prevent fraudulent activity on our platform; and for other customer service purposes. (Legal bases: performance of our contract with you; and/or our legitimate interests).

Responding to requests. To respond to your enquiries, fulfill your orders and requests. (Legal basis: performance of our contract with you).

Personalizing Content and Ads. We may use the information we collect about you to personalize the information and content we display to you, including to tailor the content and information that we may send or display to you, and to otherwise personalize your experiences while using Services, including providing you with more relevant ads. (Legal basis: our legitimate interests).

Marketing and Communications. To communicate with you about your account and use of our Services; to send you product or service, updates; to respond to your inquiries; to provide you with news, special offers, promotions, and other information we think may interest you; and for other informational, marketing, or promotional purposes. Our communications with you may include communications via email. Please see our section regarding Your Choices for more information about how to change your communications preferences. If you are located in a jurisdiction that requires opt-in consent to receive electronic marketing messages, we will only send you such messages if you opt-in to receive them. We do not use personal information to market to students or children. (Legal bases: our legitimate interests; and/or with your consent).

Research and Analytics. To analyze how you interact with our Services; to monitor and analyze usage and activity trends; and for other research, analytical, and statistical purposes. (Legal basis: our legitimate interests).

Protecting Our Legal Rights And Preventing Misuse. To protect the Site and our business operations; to prevent and detect fraud, unauthorized activities and access, and other misuse; where we believe necessary to investigate, prevent or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety or legal rights of any person or third party, or violations of our Terms of Use or this Policy. (Legal bases: our legitimate interests; and/or compliance with laws)

Complying with legal obligations. To comply with the law or legal proceedings. For example, we may disclose information in response to subpoenas, court order, and other lawful requests by regulators and law enforcement, including responding to national security or law enforcement disclosure requirements. (Legal bases: our legitimate interests; and/or compliance with laws)

Related to our general business operations: to consider and implement mergers, acquisitions, reorganizations, and other business transactions, and where necessary to the administration of our general business, accounting, recordkeeping and legal functions. (Legal bases: our legitimate interests; and/or compliance with laws)

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

Ques 3: Data Retention?

We will generally keep personal information only for as long as it remains necessary for the identified purposes or as authorized or required by law. We may retain certain data as necessary to prevent fraud or future abuse, or for legitimate business purposes, such as analysis of aggregated data, account recovery, or if required by law. All retained personal information will remain subject to the terms of this Policy.

Ques 4: What Information is being Shared?

Filter by Securly, gathers Email address and Organizational Unit from a G-Suite directory sync or by connection to Active Directory. Filter also collects Domain/URL, IP Address, Policy Names, and when configured Geolocation details.

Auditor by Securly, gathers Email address and Organizational Unit from a G-Suite directory sync or by connection to Active Directory. Auditor also stores document/email subjects and contents when they trigger categorization.

Classroom by Securly synchronizes with Google Classroom or Schoology, Classroom does not ask for any information to be directly exported from a Management Information System, but instead through an LMS (Learning Management System). The only details requested through the LMS are Email, Name, Role (Teacher/Pupil), and Class Names.

Ques 5: How Information is being Shared?

Information will be shared using TLS over HTTPS connections and is therefore encrypted in transit, for OU structure from Active Directory this is passed using the browser querying a web server within the customer network and transferring using the browser through to Securly infrastructure.

Ques 6: Data Storage and Data Security?

We store the data collected in our Cloud Database which is encrypted at rest and in transit. Securly currently serves 15,000 schools & 10M students. Over the last 7 years, we have built multiple layers of security to ensure student and children's data is protected. We have recently been audited for our data privacy handling and received a Service Organization Control (SOC) 2 audit certification - we can share a copy of this audit report. The data collected is stored in our cloud just like any other Software as a Service (SaaS) solution, but we have taken multiple measures to ensure no one at Securly has access to this data via code, configuration and policy based layered defenses.

Ques 7: Data Backup & Business Continuity ?

Backups, Restores and Availability of Data 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.

- Backups of production databases are performed based on the database type:
- Configuration - daily full snapshots/AMI backups and retained for 7 days
- Logs - monthly backups retained for one month.
- Data is replicated across geographically separate availability zones.
- Backups and replications are monitored for failures. In the event of three successive nightly failures, IT will open an incident ticket to investigate the issue.
- IT performs restorations of data per customer or business requests.
- System restore capabilities are tested at least annually

Business Continuity Planning:

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.

- Management has identified critical assets in the environment and has assessment the associated threats and vulnerabilities. See the Information Risk Management Policy for further information.
- Management has considered customer service level agreements in defining critical services and technologies for recovery.
- A team has been designated with specific roles and responsibilities to manage crisis scenarios and recovery processes.
- Recovery procedures for critical assets and functions are documented and shared with respective teams and members of leadership. Procedures include steps for notification of relevant staff and vendors, critical items to be recovered from each department, and lists of key requirement to move to an alternate worksite.

Ques 8: How the information is destroyed?

Notwithstanding the foregoing, personal information will be deleted in all cases when it is no longer needed for the purpose for which it was collected or when you terminate our services pursuant contractual agreement.

All retained personal information will remain subject to the terms of this Privacy Policy. If you would like a student's or child's personal information to be deleted, or if you would like to obtain a copy of your student's or child's personal information, please contact us at support@securly.com.

If we learn we have collected personal information about a student or child without proper consent, we will delete that information as quickly as possible. No physical copies of data will be held.

Ques 9: What is the underlying sub-service provider used by Securly to deploy production build and data center?

Amazon Web Service

Ques 10: In what geographic area(s) is the data center hosted?

US, CA, IE, UK, AU

Ques 11: How many data centers will (potentially) be used to store confidential data?

One

Ques 12: Do you allow customers to define acceptable geographical locations for data routing or resource?

Although the selection can only be made from our currently available regions/datacenters. The data center for a given customer is usually automatically assigned at the time of onboarding, where necessary this can be subject ot an override to select a more suitable location.

Ques 13: Do you use multi-factor or other Identity Management solutions to protect your infrastructure and customer data?

All Securly employees use multi-factor auth when logging into Securly systems and accessing customer data.

Ques 14: How can the users access their Data?

Access to data is via securly.com>Login>Safety Console, only authorized users can access the application to view reports and logging information or to change policies

Ques 15: Do you document how you grant and approve access to customer data?

We have recently been audited for our data privacy handling and received a Service Organization Control (SOC) 2 audit certification - we can share a copy of this audit report. The data collected is stored in our cloud just like any other Software as a Service (SaaS) solution, but we have taken multiple measures to ensure no one at Securly has access to this data via code, configuration and policy based layered defenses.

Ques 16: Who is liable for any breaches or unapproved exposure of our data?

We have a dedicated team of Devops and security engineer which ensure the data security at topmost priority. So if any breach happen a Information Security Officer will be notified and Incident Response plan is followed to limit the exposure and breach.

Ques 17: Do you have controls in place to prevent data leakage or intentional/accidental compromise between customers in a multi-customer environment?

All of our database solution are password protected. Access to these DB are limited to Devops Team only. We do perform regular vulnerability assessment to ensure that there is no vulnerability in our application which can lead to compromise of data.

Ques 18: Do you notify your customers when you make material changes to your information security and/or privacy policies?

We are SOC2 Type2 compliance so we release our SOC2 Type2 report to customer on need basis which specify the information security policy followed by Securly. Our privacy policy is

always up-to-date on https://www.securly.com/privacy page which is public accessible by customer.

Ques 19: How often agreements are reviewed?

All Agreements will be reviewed annually at time of contract expiration, or as required by customer. Agreements are reviewed by a Securly team that includes our internal legal department, our outside legal firm and the business team. Agreements are only executed (signed) by our Chief Executive Officer (CEO).

Ques 20: Data center infrastructure has been evaluated against ISO 27001?

Yes

Ques 21: Data center infrastructure has undergone an SOC 2 Type II (preferred) review.

Yes. We follow the practice for reviewing SOC2 Type2 reports of Vendor used by us. Our data center is hosted on AWS which is SOC2 Type2 Compliance.

Ques 22: Do we perform Penetration Testing?

We do internal Penetration Testing of Web application and AWS infrastructure using OWASP Guidelines. This activity is performed annually.

Ques 23: Do we perform Vulnerability Assessment?

We do internal Vulnerability assessment of instances with Nessus, Nexpose. This activity is performed Quarterly.

Ques 24: Does Application can/has the capability to use district centralized authentication such that district user can authenticate using district domain password. (e.g., SAML/ADSI/LDAP)

Yes

Ques 25: What is the password policy to login to the application?

Admin login through their district credentials so their password policy applies

Ques 26: Which encryption algorithm is used to encrypt data at rest?

AES-256 bit

Ques 27: Database and other application interface credentials are encrypted at rest and in transit.

Yes

Ques 28: Patch Management?

Our servers are on AWS Cloud which is protected via a WAF and we protect our customer from malware via malware detection feature.

Ques 29: Does Application recommends/requires any system integration.

We required Directory service (Google or Azure) integration to import OUs and SSO Authentication.

Ques 30: Does Application support role based access.

Yes

Ques 31: Application Configuration and Authorization:

- The application displays an appropriate warning message upon user login.
    - This system is for use of authorized users only.
    - Individuals using this computer system are subject to having all their activities on this system monitored and recorded.
    - Anyone using this expressly consents to such monitoring and is advised that evidence of criminal activity will be provided to law enforcement officials.

- The application does not store authentication credentials on client computers after a session terminates.
- Non-privileged users cannot perform privileged functions.
- Application users can explicitly terminate a session (logout).
- The application validates user inputs before processing them.
- The application is not vulnerable to buffer overflows as determined through the use of a "fuzz" testing tool

Ques 32: Information Security Program in case of security breach:

- Service Provider has one designated accountable party (e.g., Information Security Officer) responsible for all aspects of information security with regard to this service/application.
- Service Provider provides 7x24x365 contact for coordinating security incident efforts
- Service Provider has technology capable of and agrees to cooperate with forensic imaging requests in the event of a security incident.
- Service Provider monitors 3rd party consultants/contractors access to Service Providers data and requires an NDA (non-disclosure agreement) where applicable.
- Process: We have Security monitoring alerts that have been implemented in order to notify us in event of security breach. The Security breach is taken at P0 priority and our Security expert first validates the event efficacy. In case the event is true positive the event is informed to the information security officer and necessary action taken to remediate the event.

Ques 33: Service Level Agreement:

- Service Provider has Service Level Agreement that sets expected availability targets and penalties for noncompliance.
- Service level agreement defines data ownership throughout the lifecycle of the contract.
- Service level agreement applies to all applicable subcontractors and partners.
- Employees receive background checks before hire.
- Service Provider has Service Level Agreement that includes targets for initial response time to reports of breach of confidentiality or integrity and penalties for noncompliance.
- Service level agreement defines how information is transferred back to customer in the event of contract termination, company sale, or bankruptcy.

Ques 34: Description of Product and Services offered?

Filter

Filter is Securly's cloud-based web filtering service for schools that can filter all types of devices, whether they are school-managed or personal devices. Filter provides school administrators with features like custom policy creation, choice of more than 15 categories of content to allow or block, custom blacklists and whitelists, alerts on self-harm or bullying-related activity, and seamless Google, Azure, and Active Directory authentication using G Suite or Office 365. There are three types of Filter deployments that customers can choose from according to type of device and preference:

DNS Filter – Deployment of Filter by configuring the school networks DNS servers to point to Securly Internet Protocol (IP) addresses

Smartpac Filter – Deployment of Filter by installing Proxy auto configurations URL profiles on devices

Chrome Extension – Deployment of Filter by installing Securly's Chrome-based browser extension

Auditor

Auditor is Securly's artificial intelligence engine, which typically monitors the activity on Google Drive, Gmail, and Google Docs. It scans all the activity that students are doing on these channels and flags for self-harm and bully. Alerts detected by this engine are notified to IT Administrators at the given school, delegated administrators, principals, counselors, and parents. Important alerts are handled by Securly's 24.

Tipline

Tipline is a Securly solution that helps students and staff members to anonymously report any bullying or violent incidents. It is an easy-to-use method of sharing information about such incidents and every alert is seen and heard by Securly. The reporter can send a tip via the Tipline application, email, text, telephone, or web form.

Securly 24

Securly 24 is Securly's dedicated internal incident response team, which works 24x7 and has access to the Filter and Auditor service data. Securly 24 includes one director and seven to eight Security staff (FTE employees in the United States and in a wholly owned subsidiary in India, one FTE in the United Kingdom via a wholly owned subsidiary, and two to three contractors in Mexico. Securly 24 tracks the activities and responds to detected emergencies.

Ques 35: Who all are the end-user of of application?

Parents, School Admin, Teachers & Students

Ques 36 : What is the Data Source? How do you use the customer data?

There are various sources by which we collect the customer data:

- Directly from Customer
- Information collected at time of Registration
- Information collected via customer support
- Information collected if customer signup for newsletter and updates
- Information collected at Securly Hub purchase
- Information collected during use of our services

What all customer data we do collect and how we are going to use this:

- School Admin Email Address:
    - For Maintenance.
    - To Authenticate you as a valid customer.
    - To Respond to your queries.
    - To provide you with news, special offers, promotions, and other information we think may interest you; and for other informational, marketing, or promotional purposes
- School Admin Phone Number:
    - For Maintenance.
    - To Respond to your queries.
    - To provide you with news, special offers, promotions, and other information we think may interest you; and for other informational, marketing, or promotional purposes
- Online Activities: Site Visited, Online Searches, videos watched, email content, email address and geolocation information.
    - Used by Securly's 24 Team to detect suspicious activity performed by students.
- Our Service Usage Data.
    - To analyze how you interact with our Services; to monitor and analyze usage and activity trends; and for other research, analytical, and statistical purposes.

Ques 37: Who at company has access to customer data?

Securly's 24 Team has access to student online activity to protect them.

Only Devops Team has access to customer data.

Ques 38: Types of personal identifiable information (PII) collected; how is it collected, used and stored?

Answer:

- Admin Email Address:
  - Collected:
    - At the time of account registration
    - At the time of inquiry to support
  - Used:
    - For Maintenance.
    - To Authenticate you as a valid customer.
    - To Respond to your queries.
    - To provide you with news, special offers, promotions, and other information we think may interest you; and for other informational, marketing, or promotional purposes.
    - By Securly's 24 Team to reach out to parent in case of Self harm detection
  - Stored:
    - Information stored in transit and at rest is encrypted using SSL and AES-256 encryption respectively.
- Admin Phone Number:
  - Collected:
    - At the time of account registration
    - At the time of inquiry to support
  - Used:
    - For Maintenance.
    - To Respond to your queries.
    - To provide you with news, special offers, promotions, and other information we think may interest you; and for other informational, marketing, or promotional purposes
    - By Securly's 24 Team to reach out to parent in case of Self harm detection
  - Stored:
    - Information stored in transit and at rest is encrypted using SSL and AES-256 encryption respectively.
- Parent Email Address:
  - Collected:
    - Added by School Administrators.
  - Used:
    - To authenticate parent to parent portal.
    - For mapping between parent and child.
    - By Securly's 24 Team to reach out to parent in case of Self harm detection
  - Stored:
    - Information stored in transit and at rest is encrypted using SSL and AES-256 encryption respectively.
- Parent Phone No:
  - Collected:
    - Added by School Administrators.
  - Used:
    - By Securly's 24 Team to reach out to parent in case of Self harm detection

        - Stored:
            - Information stored in transit and at rest is encrypted using SSL and AES-256 encryption respectively.

- Student Email Address:
    - Collected:
        - Imported from School OUs
    - Used:
        - To track the student activities.
        - For mapping between parent and child.
    - Stored:
        - Information stored in transit and at rest is encrypted using SSL and AES-256 encryption respectively.
- Online Activities by Student:
    - Collected:
        - When a student used our Services.
    - Used:
        - By Securly's 24 team to protect students and do analysis to detect suspicious behavior.
    - Stored:
        - Information stored in transit and at rest is encrypted using SSL and AES-256 encryption respectively.

Ques 39: Software Encryption?

We use AES-256 bit encryption algorithm to encrypt the data at rest. All our services are deployed of HTTPS data transit on TLS protocol to ensure all the data in transit is encrypted.

Proprietary & Confidential

MDM Student Safety Suite System

SOC 2

Report on Securly's System and Organization Controls Relevant to Security

JANUARY 1, 2021 TO DECEMBER 31, 2021

Moss Adams LLP
101 Second Street, Suite 900
San Francisco, CA. 94102
(415) 956-1500

MOSSADAMS

Table of Contents

I. Independent Service Auditor's Report

Securly
111 N. Market Street, Suite 400
San Jose, CA 95113

To the Management of Securly:

Scope

We have examined Securly's accompanying description of its MDM Student Safety Suite System in Section III titled "Securly's Description of Its MDM Student Safety Suite System" throughout the period January 1, 2021 to December 31, 2021 (description) based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that Securly's service commitments and system requirements were achieved based on the trust services criteria for Security (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Securly uses the following subservice organizations:

- Amazon Web Services for hosting the Student Safety Suite and its Amazon Elastic Compute Cloud (EC2) services.
- Elastic Cloud for its distributed, real-time search and analytics engine and datastore.
- Google Workspaces for its cloud computing, productivity, and collaboration tools.

Our examination did not include the services provided by the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Securly, to achieve Securly's service commitments and system requirements based on the applicable trust services criteria. The description presents Securly's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Securly's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Securly is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Securly's service commitments and system requirements were achieved. Securly has provided the accompanying assertion in Section II titled "Securly's Assertion" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Securly is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of the controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and Securly's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether the controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of the controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of our tests are listed in Section IV of this report titled "Trust Services Category, Criteria, Related Controls, and Tests of Controls."

Opinion

In our opinion, in all material respects:

- the description presents Securly's MDM Student Safety Suite System that was designed and implemented throughout the period January 1, 2021 to December 31, 2021, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period January 1, 2021 to December 31, 2021 to provide reasonable assurance that Securly's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout that period, and if the user entities applied the complementary controls assumed in the design of Securly's controls throughout that period.
- the controls stated in the description operated effectively throughout the period January 1, 2021 to December 31, 2021 to provide reasonable assurance that Securly's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of Securly's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Securly, user entities of Securly's MDM Student Safety Suite System during some or all of the period January 1, 2021 to December 31, 2021, business partners of Securly subject to risks arising from interactions with the MDM Student Safety Suite System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and how those controls interact with the controls at the service organizations to achieve the service organizations' service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Moss Adams LLP

San Francisco, California
April 14, 2022

II. Securly's Assertion

We have prepared the accompanying description of Securly's MDM Student Safety Suite System in Section III titled "Securly's Description of Its MDM Student Safety Suite System" throughout the period January 1, 2021 to December 31, 2021 (description) based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the MDM Student Safety Suite System that may be useful when assessing the risks arising from interactions with Securly's MDM Student Safety Suite System, particularly information about system controls that Securly has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP Section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Securly uses subservice organizations:

- Amazon Web Services for hosting the Student Safety Suite and its Amazon Elastic Compute Cloud (EC2) services.
- Elastic Cloud for its distributed, real-time search and analytics engine and datastore.
- Google Workspaces for its cloud computing, productivity, and collaboration tools.

The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Securly, to achieve Securly's service commitments and system requirements based on the applicable trust services criteria. The description presents Securly's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Securly's controls.

We confirm, to the best of our knowledge and belief, that:

- the description presents Securly's MDM Student Safety Suite System that was designed and implemented throughout the period January 1, 2021 to December 31, 2021, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period January 1, 2021 to December 31, 2021 to provide reasonable assurance that the Securly service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout the period, and if the user entities applied the complementary controls assumed in the design of Securly's controls throughout that period.
- the controls stated in the description operated effectively throughout the period January 1, 2021 to December 31, 2021 to provide reasonable assurance that Securly's service commitments and system requirements were achieved based on the applicable trust services criteria, complementary user entity controls assumed in the design of Securly's controls operated effectively throughout that period.

III. Securly's Description of Its MDM Student Safety Suite System

A. Services Provided

Securly was founded in 2013 with a single intention: to keep kids safe online. The business is headquartered out of San Jose, California with offices is Charlotte, North Carolina, operations in Cancun, Mexico, and research and development in Pune, India. Securly develops solutions that keep kids safe and engaged online, at school, and at home. From tools that help adults create a kid-friendlier Internet, to an artificial intelligence that recognizes signs of bullying and even intuits risks of self-harm, Securly breaks new ground and innovates to meet modern problems head-on. For every child that we empower to stand strong, for each kid that chooses hope over hopelessness, Securly is motivated to continue forging ahead.

Securly products provide cloud-based web filtering and parental controls that works across schools and homes. Securly products prevent bullying and self-harm by generating alerts for the parents and have a service that monitors 24x7 any suspicious flags raised by the Filter and Auditor.

Securly's Student Safety Suite System represents the scope of this SOC 2 report and is comprised of:

- Filter
- Auditor
- Tipline
- Securly 24

Other solutions offered by Securly that are considered outside the scope of this report include:

- Parent Portal
- School MDM
- Chrome Tools
- PNP Hub

B. Principal Service Commitments and System Requirements

Securly designed its processes and procedures to meet its objectives for its compliance services. Those objectives are based on the service commitments that Securly makes to user entities, the law and regulations that govern the provision of its compliance services, and the financial, operational, and compliance requirements that Securly has established for the services. Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreement.

Security commitments are standardized and include, but are not limited to, the following:

- Host the production cloud infrastructure within multiple Availability Zones and Regions on Amazon Web Services (AWS)
- Encrypt the data at rest, which is stored in Elastic Cloud
- Maintain commercially reasonable administrative, technical, organizational, and physical measures to protect the security of customer data against anticipated threats or hazards
- Maintain servers in good working order with access restricted to qualified employees
- Retain the audit logs and make available as applicable
- Perform annual and quarterly vulnerability assessment and penetration testing on the application and infrastructure
- Have Securly's employees complete online information security training on annual basis
- Require third parties with access to confidential information to sign an agreement with Securly that includes requirements related to confidential information
- Maintain monitoring controls which notify Securly in case any security breaches happen to the infrastructure
- Delete all customer data within 60 days after termination

Securly establishes operational requirements that support the achievement of security commitments and other requirements. Such requirements are communicated in Securly's system policies and procedures, system design documentation, and contracts with customers. Information security polices define an organization-wide approach to how systems and data are protected.

C. Components of the System Used to Provide the Services

1. Infrastructure

AMAZON WEB SERVICES

The Platform-as-a-Service (PaaS) environments that support Securly's production environment in US East (Northern Virginia, Ohio, Northern California, and Oregon), Asia Pacific (Sydney), Canada (Central), and Europe (Ireland and London) are physically located in data centers owned and operated by AWS. AWS manages and is responsible for its own internal processes as related to the logical security of the infrastructure used by Securly. Securly also relies upon AWS for physical access controls, protection of equipment from environmental hazards, and power. Amazon Elastic Compute Cloud (EC2) is used to run and support certain elements of its application infrastructure such as filtering, cyber bulling detection, DNS service, and proxy service on the EC2 instances. Access to the services running in this infrastructure is limited through the use of Access Controls Lists (ACLs) on the security groups associated with the EC2 instances. Customer sensitive data is stored on Elasticsearch and Redis, which is maintained in AWS.

ELASTIC CLOUD

Elastic Cloud is a distributed, real-time search and analytics engine and datastore. Elasticsearch maintains all types of data, including textual, numerical, geospatial, structured, and unstructured. Securly uses Elastic Cloud to store data such as searches performed by the students on Google or Facebook. All data is encrypted at rest by Elastic Cloud.

Securly has an Elastic Cloud cluster deployed in Asia Pacific (Sydney), E.U. (Ireland), U.S. East (Northern Virginia), and US West (Oregon), with platinum support available 24x7x365. Securly has enabled the backup and recovery of Elastic Cloud to recover from any disaster.

FILES.COM

Files.com, previously known as BrickFTP, is a file sharing service used by Securly for customer file upload. Securly creates a unique username and the customer sets the password and uploads the required file. Securly receives notification once the file has been uploaded, and the uploaded data is then imported into the Securly databases.

In addition, other primary infrastructure used to provide Securly's Software-as-a-Service (SaaS) system includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Web Servers	EC2	Deploy the services that are offered to customers
Application Load Balancer	ALB, ELB, NLB	Load-balancing of EC2 clusters and services
Object Storage	S3	Storing certificates, logs, scripts, etc.
DNS Web Service	Route 53	Register Securly domain and subdomain
Relational Database	RDS MySQL Database	Relational database to maintain the customer data
IAM Console	AWS Identity Access Management	Control the access to production environment
Web Application Firewall	AWS WAF	Prevent an attack to the Securly cluster from distributed denial of service (DDoS) attacks
Auto-Scaling	AWS Auto Scaling Groups	Scale the server in peak time
Firewall	Security Groups, NACL	Firewall to ensure security of EC2 and subnets
Compliance Scanning	AWS Config	Compliance scanning of identity and access management (IAM) resources
Security Alerting	AWS GuardDuty	Alerting if any critical malicious activity is detected in the infrastructure

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Logging & Monitoring	CloudWatch, CloudTrail	Logging CPU, memory utilization, and as an alerting engine in case of any emergency
Serverless Computing	Lambda	Execute application features and process
Email Notification	SES, SNS	Notification service to alert in case of any emergency situation
NoSQL Database	Elasticsearch	Store the activity of the students
Code Deployment	CodeDeploy	Configuration management tool and to deploy the code in production environment.
Cache	Elastic Cache	Host Redis so that frequently required data can be accessed immediate.
Certificate Management	Certificate Manager	Manage the SSL certificates of Securly.

2. Software

Securly's Student Safety Suite System represents the scope of this SOC 2 report and is comprised of:

- Filter
- Auditor
- Tipline
- Securly 24

FILTER

Filter is Securly's cloud-based web filtering service for schools that can filter all types of devices, whether they are school-managed or personal devices. Filter provides school administrators with features like custom policy creation, choice of more than 15 categories of content to allow or block, custom blacklists and whitelists, alerts on self-harm or bullying-related activity, and seamless Google, Azure, and Active Directory authentication using G Suite or Office 365. There are three types of Filter deployments that customers can choose from according to type of device and preference:

- *DNS Filter* – Deployment of Filter by configuring the school networks DNS servers to point to Securly Internet Protocol (IP) addresses
- *Smartpac Filter* – Deployment of Filter by installing Proxy auto configurations URL profiles on devices
- *Chrome Extension* – Deployment of Filter by installing Securly's Chrome-based browser extension

AUDITOR

Auditor is Securly's artificial intelligence engine, which typically monitors the activity on Google Drive, Gmail, and Google Docs. It scans all the activity that students are doing on these channels and flags for self-harm and bullying. Alerts detected by this engine are notified to IT Administrators at the given school, delegated administrators, principals, counselors, and parents. Important alerts are handled by Securly's 24.

TIPLINE

Tipline is a Securly solution that helps students and staff members to anonymously report any bullying or violent incidents. It is an easy-to-use method of sharing information about such incidents and every alert is seen and heard by Securly. The reporter can send a tip via the Tipline application, email, text, telephone, or web form.

SECURLY 24

Securly 24 is Securly's dedicated internal incident response team, which works 24x7 and has access to the Filter and Auditor service data. Securly 24 includes one director and seven to eight Security staff (FTE employees in the United States and in a wholly owned subsidiary in India, one FTE in the United Kingdom via a wholly owned subsidiary, and two to three contractors in Mexico). Securly 24 tracks the activities and responds to detected emergencies.

In addition to the Student Safety Suite System, Securly uses the following software systems:

Primary Software	
Software	**Purpose**
Apache Server	Used to host Securly's website
CMS	Used as content management software to build websites
Confluence	Used for maintaining Securly's documents
ElasticCloud	Used to store the student activities that they perform online
Elasticsearch	Used to store the online activities performed by student
Files.com	Used as an FTP server by which customer can share the file to upload parent and student relationship
Firebase	Used for managing mobile app push notifications
Fluentd	Used for shipping user logs to the Elasticsearch database and for triggering AWS lambda events
GitHub	Used as a Code Repository Management
Google	Used for G Suite system and services
G Suite	Used as email, documentation, and maintaining organizational units (OUs)
IPvsdm	Used for IP forwarding
Jenkins	Used by DevOps for automation build deployment and infrastructure creation
JIRA	Used for internal communication and managing the releases, requirements, and tasks
Maxmind	Used for getting IP databases for different geographical regions, which helps to know content on websites based on user geographical location
Monit	Used to monitor the services running on cluster and give PagerDuty alerts
MySQL	Used to store the customer relational data

Primary Software	
Software	**Purpose**
Nagios Logger	Used for monitoring application logs
OpenVPN	Used to provide VPN services to employees
Redis	Used as cache to access the customer data
RingCentral	Used as internal/external conferencing and meeting tool
Rsyslogng	Used for pushing application logs to centralize syslog server
Salesforce	Used for customer support management
Sendy	Used for sending marketing campaign emails
Slack	Used for live discussion as an internal messenger
Splunk	Used to store the student activities that they perform online
Squid Proxy	Used as a proxy to filter the traffic of students activity online
Stack-Driver	Used as a monitoring tool
Unbound	Used as DNS routing to route the traffic to Squid Proxy
VividCortex	Used as a database monitoring tool
Zendesk	Used as a support ticketing tool

3. People

A Board of Directors is in place and oversees management activities. Reporting to the Board of Directors, the Chief Executive Officer and the Chief Revenue Officer are responsible for the overall operation of Securly. The Board of Directors meets quarterly and is consulted and involved in all significant business decisions.

Reporting to the Chief Executive Officer and the Chief Revenue Officer, each member of the senior management team has a distinct, separate responsibility within the organization. Roles and responsibilities have been segregated to the extent possible and a formal organization chart has been developed.

Securly's senior management report directly to the Chief Executive Officer and is listed below:

- Chief Design Officer
- Senior Vice President of Customer Success
- Senior Vice President of Engineering – India
- Senior Vice President of Finance
- Senior Vice President of Sales Operations
- Senior Vice President of Sales
- Senior Vice President of Customer Success
- Vice President of Support
- General Manager of CLT Operations
- General Manager of Classroom and MDM

Securly, Inc. currently has a staff of approximately 160 employees. Roles and responsibilities have been segregated to the extent possible and a formal organization chart has been developed, containing the following main departments (alphabetical order):

- Engineering
- G&A (Finance, HR, etc.)
- Marketing
- Sales
- Support

SENIOR LEADERSHIP TEAM

Overseen by Chief Executive Officer, the Senior Leadership team is responsible for overseeing company-wide activities, establishing, accomplishing goals, marketing, public, analyst relations, account management, engineering implementations, customer support, forging key strategic partnerships, managing the recruiting, hiring, human resources operations of the company, sales, managing the fiscal and day to day operations of the company.

ENGINEERING

Engineering is responsible for developing, testing, deploying, maintaining, and securing software and infrastructure for Securly production applications. These responsibilities are shared among the multiple global teams within Engineering. The teams and their responsibilities are as follows:

- *Software Development* – Responsible for developing the software for the Securly applications, as well as making improvements and enhancements to it per the business needs.
- *Quality Assurance* – Responsible for testing new software, reporting issues with new software, and tracking them to resolution.
- *Project Management* – Responsible for tracking and managing planned infrastructure and software projects, ensuring projects meet deadlines and objectives.

- *DevOps* – Responsible for the build and release of new software, managing the security of Securly's production applications and infrastructure, making changes to production servers, infrastructure, and configurations, ensuring overall availability and reliability of the system, and granting and revoking logical access to systems within Securly production network and infrastructure.
- *Data Team* – Responsible for analyzing data and providing data to internal teams for marketing, decision-making, and engineering projects.

SUPPORT

Support is responsible for providing support services to the customers and employees. Support consists of customer support, 24 student safety support, and the IT team.

- *Customer Support* – Responsible for providing technical support to customers through a cloud-based ticketing system and communicating information to customers regarding new issues and/or developments.
- *24 Student Safety Support* – Responsible for alerting schools and 911 about suspicious student activity related to self-harm or bullying.
- *IT Support* – Responsible for managing corporate computing devices, business applications, logical access to internal communication applications and email, supporting toolsets, and employee and contractor identities.
- *Product Management* – Responsible for building features and products for customers, as well as actively communicating the changes to external and internal stakeholders such as customers and employees.
- *Human Resources* – Responsible for onboarding new personnel, defining the role/position of new hires, performing background checks, and administering physical access to Securly corporate offices, and facilitating the employee termination process.

EXTERNAL USERS

The following are the external users that are given access to the system based on their assigned roles and responsibilities at a given school.

- *IT Administrator* – A dedicated IT Administrator can login to the Admin Portal and can access all the features to view the student activities, get the alerts about suspicious behavior of student, and apply the filter policy.
- *Delegated Administrator* – Created by an IT Administrator, a Delegated Administrator is a user that can be any staff member of a school given limited access to the Admin Portal to monitor the student activities within a school.
- *Parents* – Parents can login to the Parent Portal to view their children's activities at school or at home. Parents can also apply settings for what their children can view online.

4. Data

INFORMATION ASSET

Critical production information assets are hosted by AWS. Through the management console, Securly has access to a complete and accurate inventory of current assets used to support the production environment.

DATABASES

Three databases are in use by Securly. These include:

- *Elasticsearch* – Contains all student data. All student online data is logged to Elasticsearch.
- *MySQL* – Infrastructure defers from one cluster to another (moving to EC2 to RDS). Stores all student and school-related data.
- *Redis* – Used as cache for performance and access, containing the data needed to make a filtering decision.

DATA STORAGE

The company has established means of securely storing data according to the classification.

- Restricted and Confidential data is stored using AES 256-bit encryption when stored on any media type.
- Access to cryptographic keys is restricted.
- Public information can be stored on any company computer.
- Hard copies of Restricted or Confidential information must be secured in a locked drawer or file cabinet.
- All Personal Identification Information (PII) is stored on Elasticsearch.
- All associated data device and associated users' device locations and parent student relations is stored in MySQL and Redis.

DATA COMPLIANCE

Securly maintains compliance with the Family Educational Rights and Privacy Act (FERPA).

DATA CLASSIFIED

Securly has established criteria for determining how data sets and information within the environment should be used, handled, and protected, based on their content and level of sensitivity to the business and the company's customers.

Management has identified the following data types:

- *Restricted* – Highly sensitive data that if compromised could put the company at financial or legal risk, may be subject to state/federal/international privacy regulations, Personally Identifiable Information (PII), Personal Health Information (PHI), credit card information, intellectual property (IP), and Social Security Numbers (SSNs)
- *Confidential* – Sensitive data that if compromised would negatively affect the operations or reputation of the company (performance reviews, vendor contracts, trade secrets)
- *Private* – Data that should only be disclosed to employees and authorized vendors and third parties of the company, not appropriate for public disclosure (organizational charts, employee contact information, sales strategy, employee handbooks)
- *Public* – Data that may be freely disclosed to the public (approved marketing materials, contact information, product pricing details)

DATA TRANSMISSION

The company has established means of securely transmitting data according to the classification using cryptography and other security protocols.

- The company uses transport layer security protocols for web and email communications.
- Restricted information cannot be shared over open public wireless networks.

DATA RETENTION

Securly has established a schedule to retain data according to legal and regulatory mandates and to meet the company's SLAs and commitments. Personal data is kept no longer than necessary for the purposes for which it is being processed.

- Information must be stored for at least one year from the date of collection.
- The data and records retention schedule is reviewed annually for ongoing compliance.
- Exceptions to the retention policy must be requested by the relevant business unit and approved by management.

DATA DISPOSAL

Securly has established a schedule to dispose of data according to legal and regulatory mandates, and to meet the company's service level agreements and commitments. Customer Service and Support teams will notify the DevOps team of a customer request to terminate their service. Restricted and Confidential customer data is permanently deleted within 60 days of the customer request.

5. Processes and Procedures

Securly has documented policies and procedures to support the development, operations, maintenance, and monitoring of controls over its physical and logical environments. The policies and procedures are in place so that the systems remain secure and available, information is kept confidential and private, and the integrity of processing is upheld. Specific relevant policies include the following:

INFORMATION SECURITY POLICY

This suite of policies and procedures addresses various components of information security that have been developed to protect Securly's critical assets, data, staff, and customers. Employees are required to acknowledge that they understand and will adhere to the policies. Key topics addressed by the policy include:

- Acceptable Use Policy
- Use and Protection of Mobile Devices
- Physical Security
- Employee Communication and Training
- Anti-Virus and Anti-Malware
- Intrusion Detection System
- Penetration Testing

SOFTWARE DEVELOPMENT LIFECYCLE POLICY

This suite of policies and procedures shows how Securly manages the design, development, testing, and deployment of software. Key topics addressed by the policy include:

- Design and Development
- Testing
- Approvals
- Deployment
- Emergency Procedures

THIRD-PARTY AND VENDOR MANAGEMENT POLICY

This document is intended to assist management and process owners in performing and monitoring activities pertaining to the management of risk associated with the use of vendors and third parties. Key topics addressed by the policy include:

- New Vendor Setup
- Service Level Agreements
- Third-Party Risk Management

DATA CLASSIFICATION AND HANDLING POLICY

This document is intended to assist management and process owners in performing and monitoring activities pertaining to the classification and handling of data and information in order to meet the company's system requirements and service commitments.

Key topics addressed by the policy include:

- Information Assets
- Data Storage
- Classification of Data Types
- Data Transmission
- Data Retention
- Data Disposal

ACCESS AND AUTHENTICATION POLICY

This document is intended to assist management and process owners in performing and monitoring activities performed to manage the risk associated with unauthorized access to information. Key topics addressed by the policy include:

- New or Modified Access
- Authentication
- User Access Review
- Deprovisioning

- Administrative and Privilege Access
- Shared and Generic Accounts

BUSINESS CONTINUITY AND DISASTER RECOVERY POLICY

This document is intended to assist management and process owners in performing and monitoring activities pertaining to the disaster recovery plans and business continuity program in order to meet the company's system requirements and service commitments. Key topics addressed by the policy include:

- Backups, Restoration, and Availability of Data
- Business Continuity Planning
- Annual Testing

INCIDENT MANAGEMENT AND RESPONSE POLICY

This document is intended to assist management and process owners in performing and monitoring activities pertaining to the identification and resolution of security incidents. Key topics addressed by the policy include:

- Incident Monitoring and Identification
- Incident Tracking and Classification
- Containment, Eradication, and Recovery
- Root Cause Analysis

INFORMATION RISK MANAGEMENT POLICY

This document is intended to assist management and process owners in performing and monitoring activities pertaining to the management of risks associated with the company's ability to meet system requirements and service commitments. Key topics addressed by the policy include:

- Internal Risk Assessment
- External Risk and Control Assessment
- Other Information Risk Management Activities

PATCHING AND VULNERABILITY MANAGEMENT POLICY

This document is intended to assist management and process owners in performing and monitoring activities pertaining to the management of security vulnerabilities in order to meet the company's system requirements and service commitments.

Key topics addressed by the policy include:

- Patching
- Vulnerability Scanning
- Reporting, Prioritizing, and Remediation
- Penetration Testing

D. Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

1. Control Environment

MANAGEMENT CONTROL

Securly has established appropriate lines of reporting, which facilitate the flow of information to appropriate people in a timely manner. Roles and responsibilities are segregated based on functional requirements. Securly has an organization chart that defines the organizational structure and reporting lines. Responsibility for the design, development, implementation, maintenance, and monitoring of Securly's security policies has been assigned to the DevOps team. They perform routine updates as technology, industry, regulatory, and business requirements change. The ultimate responsibility of the overall information security is the responsibility of the Chief Executive Officer and the Director of Operations.

A third party performs a background check on all new employees and contractors. This includes an employment check, criminal records check, county records check, SSN trace, and national criminal and sex offender check.

Access to the new employee is requested through an access request form that is approved by the employee's manager.

Management performs the review of subservice organizations by reviewing their SOC 2 reports, and any exceptions noted are addressed. This includes for AWS, Elastic Cloud, and Google.

Any change to the production environment is approved by management, and DevOps is the only one who can make modification to production environment.

SECURITY MANAGEMENT

The Securly security process is described in the Information Security Policy, which consists of following:

- Acceptable Use Policy
- Use and Protection of Mobile Devices
- Physical Security
- Employee Communication and Training
- Anti-Virus and Anti-Malware
- Intrusion Detection System
- Penetration Testing

Securly keeps customer information confidential and data up-to-date and error-free. Securly also keeps systems well-managed, replete with operating system updates, security patches, and with limited access to licensed customers, authorized employees, and contractors.

As a part of security efforts, Securly uses several strategies to detect issues such as:

- Logging user access to any activity on AWS accounts.
- Tracking any modification to the security group with public access.
- Logging work performed on production servers using CloudTrail.
- Tracking vulnerabilities and updates related to the server's operating system and applications.
- Tracking uptime related to the SLAs or other services to the customers.
- Maintaining the Security Charter where quarterly goals for the Security team have been identified and aligned to the roadmap.

In addition, Securly conducts internal web application assessment and penetration testing of production infrastructure and web applications allowing the opportunity to detect more complex security issues within products.

SECURITY POLICIES

Securly has designed several policies to protect the security of the systems, the privacy of customer data, and internal confidential information related to the ability to calculate applicable plans and rates for quotes and proposals. These security policies include:

- *Information Security Policy* – Records policies and procedures for how Securly plans to implement high level information security protections within the organization, including definitions, procedures, and responsibilities.
- *Patching and Vulnerability Management Policy* – Records policies and procedures for how Securly plans to prevent, identify, classify, and accordingly handle vulnerabilities to information assets in the environment.
- *Information Risk Management Policy* – Records policies and procedures for how Securly plans to develop, manage, and control vendor and third-party contracts, relationships, and performance.
- *Incident Management & Response Policy* – Records policies and procedures for how Securly plans to detect and respond to events in the environment that could impact the security of the system and the company's ability to meet its system requirements and service commitments.
- *Access & Authentication Policy* – Records policies and procedures for how Securly plans to manage and control access to information assets to minimize the risk of inappropriate access to data resulting in data loss.
- *Data Classification and Handling Policy* – Records policies and procedures for how Securly plans to identify, classify, and accordingly handle information assets (data) within the environment.

CHANGE MANAGEMENT

Securly uses a Change Management and Software Development Policy to direct change management practices.

DESIGN AND DEVELOPMENT

Securly has established a process to obtain necessary inputs, documentation, and approvals for the creation of updates. The design and development process includes:

- The design and details of all changes to the software must be documented, proposed, and signed off prior to initiating development processes.
- Change specifications are documented to record necessary information including critical issues, system impairments, customer impacts, etc.
- Once the design approval is documented, the responsible Developer creates the new features in their own test environment.

TESTING

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. The testing process includes:

- A risk analysis is performed by the team overseeing the creation of a change or new feature (Developer, Quality Assurance, and Project Manager).
- All changes and new features are tested by a Quality Assurance tester who provides approval that the update has completed testing.
- Quality Assurance testing is performed in a separate environment that is similar to the production environment.
- An impact analysis is performed and documented upon completion of testing.

APPROVALS

Management has implemented a series of required approvals for any changes to the production environment, supporting products, and services. The approvals process includes:

- In addition to design and quality assurance approvals, deployment approvals are required by relevant stakeholders and recorded in the ticketing system prior to deployment.
- If the change is owned and managed by the DevOps team, additional deployment approval is required by the DevOps manager.
- No further changes to the release are permitted after approval.

DEPLOYMENT

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. The deployment process includes:

- Upon receipt of deployment approvals, the change is passed to the Build and Release team within the DevOps team. Access to deploy to production is restricted to members of the Build and Release team, who do not perform development activities.
- Releases are initially deployed to the beta environment, where impact is limited to a small number of customers.
- The Build and Release team monitors the success of the Beta deployment. If no risks or issues are identified, the team continues to deploy the update on a cluster-by-cluster basis, starting with the least populated clusters.

EMERGENCY PROCEDURES

To ensure that processes are in place to quickly respond to customer or internal incidents that require updates to product code or other production environments, management has established procedures for alternative change controls when individuals or teams are not immediately available for timely response. The emergency procedures include:

- In the event of an unplanned event, typically triggered by system impairment, unexpected events from code deployment, or customer-facing downtime, a Priority 0 ticket is created to track the resolution of the issue.
- If the issue is known to be customer-facing, customers on the affected clusters are notified that they are going into safe mode, which limits their functionality, but prevents downtime while triaging and resolving issues.
- Stakeholders are alerted to the identified issue and the DevOps team gets on a call to triage the issue and create a solution.
- Based on the issue, the team rolls back any necessary deployed code.
- Updates and/or fixes are developed and sent directly to Quality Assurance for testing. Quality Assurance specifically tests for implementation of the needed fix. The updates/fixes are deployed to production once Quality Assurance testing is complete.
- A root cause analysis is performed and documentation regarding the details of the change and its necessary approvals is captured within 48 hours of deployment.

DATA BACKUP AND RECOVERY

Securly ensures that the services and operations of Securly can be restored within a defined timeframe in the case of any disaster.

Securly has defined the backup and recovery test plan, which consists of taking backup and testing their restoration annually. Customer and production data is backed up on a nightly basis for MySQL and Redis databases, while Elasticsearch data is backed up on a weekly basis.

Recovery procedures are documented and available to support restores as needed, and the procedures are tested annually.

2. Risk Assessment Process

Leadership and management have implemented a process for identifying, analyzing, and addressing relevant risks and aligning them with the annually developed organizational strategy and objectives.

Securly's risk assessment process identifies and manages risks that could potentially affect Securly's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility.

Securly identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

Securly has established an independent organizational business unit that is responsible for identifying risks to the Securly and monitoring the operation of the company's internal controls. The approach is intended to align Securly's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Securly attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

RISK ANALYSIS

Risk analysis is an essential process to Securly's success. It includes identification of key business processes where potential exposures of some consequence exist, as well as significant changes to those processes. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring, and identification of the control activities necessary to mitigate the risk. Management has identified these control activities and documented them in the Trust Services Category, Criteria, and Related Controls section below. Additionally, management reviews the assessed risk levels on an annual basis and documents the risk assessment in the annual risk program.

POTENTIAL FOR FRAUD

Management considers the potential for fraud when assessing the risks to the company's objectives. The potential for fraud can occur in both financial and non-financial reporting. Other types of fraud include the misappropriation of assets and illegal acts such as violations of governmental laws. Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. Therefore, documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process. Additionally, the risk assessment that is performed on an annual basis, considers the potential for fraud.

RISK MITIGATION

Policies and procedures are in place to guide personnel in risk mitigation activities, including monitoring processes and development of policies, procedures, and communications to meet Securly's objectives during response, mitigation, and recovery efforts. Security stakeholders perform a risk assessment on an annual basis that includes an evaluation of risk mitigation control activities for risks arising from potential business disruptions. Disaster recovery and business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. The plans are reviewed, updated, and approved annually based on the business impact analysis during the annual risk assessment process. The organization obtains insurance to offset financial impact of a risk materializing.

A Third Party and Vendor Management Policy is in place that addresses the following:

- Specific requirements for a vendor and business partner
- Due diligence process prior to accepting new vendors or business partners
- Monitoring process to review vendor and business partner compliance on a periodic basis
- Exception handling
- Termination of contract

PROPRIETARY AND CONFIDENTIAL

All policies are reviewed and updated as needed during the annual risk assessment process.

Vendors are evaluated in accordance with the vendor screening process and approved by management prior to processing customer data. Signed nondisclosure agreements of confidentiality and protection are required before sharing information designated as confidential with third parties. The Senior Leadership team reviews vendor audit reports on at least an annual basis to ensure that third-party providers are in compliance with the organization's requirements.

INTEGRATION WITH RISK ASSESSMENT

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently.

Securly assigns owners to each risk identified during the annual risk assessments, and those owners are responsible for selecting and developing the control activities to mitigate those risks.

3. Information and Communication Systems

Information and communication are integral parts of Securly's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time necessary to conduct, manage, and control Securly's operations.

INTERNAL COMMUNICATION

Securly has implemented various methods of communication to ensure significant events are communicated internally in a timely manner. These methods include company meetings, information sessions, and the use of electronic mail messages to communicate time-sensitive information and Slack-channels to have internal communication.

Securly uses below software for internal communication:

- *JIRA* – Ticketing tool used to track and assign ownership of activities by the DevOps and Engineering teams. JIRA is also used to create support tickets for issues escalated by customers through the Customer Support team and allows for management to monitor and track progress of projects.
- *Slack* – For any live discussion and as internal messenger employee uses Slack.
- *Email* – All important communication happens over email.

EXTERNAL COMMUNICATION

All external communications are handled via Salesforce and Zendesk, and the responsibility for such commitments reside with the Sales/Customer Success team for Salesforce and the Support team of Securly for Zendesk. The Customer Success team uses email to communicate with customers, while the Sales team uses Salesforce, phone calls, and email to communicate with customers.

4. Monitoring Controls

Monitoring of internal controls is a critical aspect in evaluating whether controls are operating as intended and whether they are appropriately modified to reflect the changes in the control environment. Management is responsible for monitoring the quality of internal control performance as a routine part of their activities. Quarterly Security team meetings take place where critical issues are identified and corrective actions are discussed and prioritized based on risk. Additionally, Securly performs internal assessments of their security and availability controls.

The services provided by AWS, Elastic Cloud, Slack, and Atlassian are monitored on a regular basis as part of the day-to-day operations. As they become available, Securly personnel receive and review documentation (SOC reports and/or security certifications) provided by these organizations to help ensure security practices are being followed.

The following are monitoring tools used by Securly:

- *AWS CloudTrail and AWS Config* – Securly has configured an alerting notification in case of any modification to access controls, and uses AWS CloudTrail and AWS Config maintain compliance of access controls and other AWS services.
- *AWS GuardDuty* – Securly uses AWS GuardDuty as a security incident monitoring tool to continuously analyze the DNS and VPC logs. Any malicious incident is notified to Securly's Security team via email notification.
- *CloudWatch* – Securly uses CloudWatch to monitor the CPU and memory utilization of the EC2 instances. It is also used to alert the DevOps team of any suspicious activity if resources become unavailable.

- *Monit* – Monit is the service used by Securly to get PagerDuty alerts if any of the services running on the EC2 instances go down.
- *VividCortex* – Securly uses VividCortex for database monitoring, which typically includes the query running time and database deadlock. VividCortex also helps in monitoring which query runs the most.

E. Trust Services Criteria and Related Controls

Although the applicable trust services criteria, related controls, and management responses to deviations, if any, are presented in Section IV of this report titled "Trust Services Category, Criteria, Related Controls, and Tests of Controls", they are an integral part of Securly's system description throughout the period January 1, 2021 to December 31, 2021.

F. Complementary User Entity Controls

Securly's MDM Student Safety Suite System was designed under the assumption that certain controls would be implemented by the user entities for whom it provides its MDM Student Safety Suite System. In these situations, the application of specific controls at these customer organizations is necessary to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

This section describes additional controls that should be in operation at the customer organizations to complement the controls at Securly. User auditors should consider whether the following controls have been placed in operation by the customers.

Each customer must evaluate its own internal control structure to determine if the identified customer controls are in place. Users are responsible for:

Complementary User Entity Controls	
1	Understanding and complying with their contractual obligations to Securly.
2	Provisioning and removing access to their Securly instances in a secure manner.
3	Ensuring that only authorized users have access to their Securly instances.
4	Notifying Securly in the event of a suspected or known security issue or breach
5	Maintaining their own systems of record.
6	Allowing only authorized personnel to know and understand the services, network, and supporting infrastructure of Securly.
7	Developing their own disaster recovery and business continuity plans which addresses the inability to access or utilize Securly's services.

IV. Trust Services Category, Criteria, Related Controls, and Tests of Controls

This SOC 2 Type 2 Report was prepared in accordance with the AICPA attestation standards, and has been performed to examine the suitability of the design and operating effectiveness of controls to meet the criteria for the Security category set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) throughout the period January 1, 2021 through December 31, 2021.

The trust services category for the Security criteria and related controls specified by Securly are presented in Section IV of this report.

Test procedures performed in connection with determining the operating effectiveness of controls detailed here in Section IV are described below:

Test Procedure	Description
Inquiries	Inquiry of appropriate personnel and corroboration with management.
Observation	Observation of the application, performance or existence of the control.
Inspection	Inspection of documents and reports indicating performance of the control.
Reperformance	Reperformance of the control.

APPLICABLE TRUST SERVICES CRITERIA RELEVANT TO SECURITY

Common Criteria

CC 1.0 Control Environment				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 1.1	The entity demonstrates a commitment to integrity and ethical values.	The Information Security Policy posted on Google Drive specifies which roles have authority and responsibilities over aspects of the system. In addition, the policy covers integrity and ethics. The Information Security Policy is reviewed and updated on an annual basis.	Inquired of the Senior DevOps Engineer about the Information Security Policy noting that the Information Security Policy posted on Google Drive specified which roles had authority and responsibilities over aspects of the system. Noted that the policy covered integrity and ethics. Also noted that the Information Security Policy was reviewed and updated on an annual basis. Inspected the Information Security Policy and its location on Google Drive noting that the Information Security Policy posted on Google Drive specified which roles had authority and responsibilities over aspects of the system. Noted that the policy covered integrity and ethics. Also noted that the Information Security Policy was reviewed and updated on an annual basis.	No exceptions noted. No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Securly's employees and contractors are required to complete online Information Security Training on an annual basis. Topics include security, compliance, data leakage, technology trends, and acknowledgement of the Information Security Policy.	Inquired of the IT Specialist about security training noting that Securly's employees and contractors were required to complete online Information Security Training on an annual basis. Also noted that topics included security, compliance, data leakage, technology trends, and acknowledgement of the Information Security Policy. Inspected the Information Security Training documentation noting that topics included security, compliance, data leakage, technology trends, and acknowledgement of the Information Security Policy. Inspected the Information Security Training certificate and Information Security Policy acknowledgement for randomly selected current employees and contractors during the examination period noting that Securly's employees and contractors were required to complete online Information Security Training on an annual basis and acknowledge the Information Security Policy.	No exceptions noted. No exceptions noted. No exceptions noted.
		Management monitors employee performance throughout the year, and in instances where performance does not meet expectations a formalized performance improvement plan is documented within the employee's personnel file.	Inquired of the Head of Talent Acquisition about employee performance monitoring noting that Management monitored employee performance throughout the year, and in instances where performance did not meet expectations a formalized performance improvement plan was documented within the employee's personnel file. Inspected the performance improvement plans for each current employee that was subject to a performance improvement plan during the examination period noting that management monitored employee performance throughout the year, and in instances where performance did not meet expectations a formalized performance improvement plan was documented within the employee's personnel file.	No exceptions noted. No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	An independent Board of Directors oversees risks to Securly and meets on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and General Data Protection Regulation (GDPR).	Inquired of the Director of Engineering about the Board of Directors noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR. Inspected Board meeting minutes noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR.	No exceptions noted. No exceptions noted.
		The Bylaws guide the Board of Directors to demonstrate independence from management and exercise oversight of the Company.	Inquired of the Senior DevOps Engineer about the Board of Directors noting that the Bylaws guided the Board of Directors to demonstrate independence from management and exercise oversight of the Company. Inspected the Board of Directors Bylaws noting that the Bylaws guided the Board of Directors to demonstrate independence from management and exercise oversight of the Company.	No exceptions noted. No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	An independent Board of Directors oversees risks to Securly and meets on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and General Data Protection Regulation (GDPR).	Inquired of the Director of Engineering about the Board of Directors noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR. Inspected Board meeting minutes noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR.	No exceptions noted. No exceptions noted.
		Securly has an organizational chart which outlines the structure of the organization including reporting lines, authorities, and assigned responsibilities. The organization chart is maintained by the Manager of Operations, overseen by the Chief Executive Officer, and resides in a standalone Google Drive directory.	Inquired of the Senior DevOps Engineer about the organization structure noting that Securly had an organizational chart which outlined the structure of the organization including reporting lines, authorities, and assigned responsibilities. Also noted that the organization chart was maintained by the Manager of Operations, overseen by the Chief Executive Officer, and resided in a standalone Google Drive directory. Inspected the organizational chart and its location noting that Securly had an organizational chart which outlined the structure of the organization including reporting lines, authorities, and assigned responsibilities. Also noted that the organization chart was maintained by the Manager of Operations, overseen by the Chief Executive Officer, and resided in a standalone Google Drive directory.	No exceptions noted. No exceptions noted.
		Roles and responsibilities related to security are defined in written job descriptions.	Inquired of the IT Specialist about job descriptions noting that roles and responsibilities related to security were defined in written job descriptions. Inspected the job descriptions for randomly selected new employees during the examination period noting that roles and responsibilities related to security were defined in written job descriptions.	No exceptions noted. No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A background check is performed on all new employees and contractors. Employment is contingent on successful completion of a background check that includes a reference check, employment check, and criminal records check that must be completed within a 90-day probationary period.	Inquired of the IT Specialist about background checks noting that a background check was performed on all new employees and contractors. Also noted that employment was contingent on successful completion of the background check that included a reference check, employment check, and criminal records check that must be completed within the 90- day probationary period.	No exceptions noted.
			Inspected the background check for randomly selected new employees during the examination period noting that a background check was performed on new employees. Also noted that employment was contingent on successful completion of the background check that included a reference check, employment check, and criminal records check that must be completed within the 90- day probationary period.	No exceptions noted.
			Inspected the background check for randomly selected new contractors during the examination period noting that a background check was performed on new contractors. Also noted that employment was contingent on successful completion of the background check that included a reference check, employment check, and criminal records check that must be completed within the 90-day probationary period.	No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		New employees and contractors are required to read and acknowledge Securly's Non-Disclosure Agreement (NDA) as part of the hiring process.	Inquired of the IT Specialist about the NDA noting that new employees and contractors were required to read and acknowledge Securly's NDA as part of the hiring process.	No exceptions noted.
			Inspected the signed NDAs for randomly selected new employees during the examination period noting that new employees were required to read and acknowledge Securly's NDA as part of the hiring process.	No exceptions noted.
			Inspected the signed NDA for randomly selected new contractors during the examination period noting that new contractors were required to read and acknowledge Securly's NDA as part of the hiring process.	No exceptions noted.
		Securly's employees and contractors are required to complete online Information Security Training on an annual basis. Topics include security, compliance, data leakage, technology trends, and acknowledgement of the Information Security Policy.	Inquired of the IT Specialist about security training noting that Securly's employees and contractors were required to complete online Information Security Training on an annual basis. Also noted that topics included security, compliance, data leakage, technology trends, and acknowledgement of the Information Security Policy.	No exceptions noted.
			Inspected the Information Security Training documentation noting that topics included security, compliance, data leakage, technology trends, and acknowledgement of the Information Security Policy.	No exceptions noted.
			Inspected the Information Security Training certificate and Information Security Policy acknowledgement for randomly selected current employees and contractors during the examination period noting that Securly's employees and contractors were required to complete online Information Security Training on an annual basis and acknowledge the Information Security Policy.	No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Roles and responsibilities related to security are defined in written job descriptions.	Inquired of the IT Specialist about job descriptions noting that roles and responsibilities related to security were defined in written job descriptions. Inspected the job descriptions for randomly selected new employees during the examination period noting that roles and responsibilities related to security were defined in written job descriptions.	No exceptions noted. No exceptions noted.
		New employees and contractors are required to read and acknowledge Securly's Non-Disclosure Agreement (NDA) as part of the hiring process.	Inquired of the IT Specialist about the NDA noting that new employees and contractors were required to read and acknowledge Securly's NDA as part of the hiring process. Inspected the signed NDAs for randomly selected new employees during the examination period noting that new employees were required to read and acknowledge Securly's NDA as part of the hiring process. Inspected the signed NDA for randomly selected new contractors during the examination period noting that new contractors were required to read and acknowledge Securly's NDA as part of the hiring process.	No exceptions noted. No exceptions noted. No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Securly's employees and contractors are required to complete online Information Security Training on an annual basis. Topics include security, compliance, data leakage, technology trends, and acknowledgement of the Information Security Policy.	Inquired of the IT Specialist about security training noting that Securly's employees and contractors were required to complete online Information Security Training on an annual basis. Also noted that topics included security, compliance, data leakage, technology trends, and acknowledgement of the Information Security Policy. Inspected the Information Security Training documentation noting that topics included security, compliance, data leakage, technology trends, and acknowledgement of the Information Security Policy. Inspected the Information Security Training certificate and Information Security Policy acknowledgement for randomly selected current employees and contractors during the examination period noting that Securly's employees and contractors were required to complete online Information Security Training on an annual basis and acknowledge the Information Security Policy.	No exceptions noted. No exceptions noted. No exceptions noted.
		Management monitors employee performance throughout the year, and in instances where performance does not meet expectations a formalized performance improvement plan is documented within the employee's personnel file.	Inquired of the Head of Talent Acquisition about employee performance monitoring noting that Management monitored employee performance throughout the year, and in instances where performance did not meet expectations a formalized performance improvement plan was documented within the employee's personnel file. Inspected the performance improvement plans for each current employee that was subject to a performance improvement plan during the examination period noting that management monitored employee performance throughout the year, and in instances where performance did not meet expectations a formalized performance improvement plan was documented within the employee's personnel file.	No exceptions noted. No exceptions noted.

CC 2.0 Communication and Information				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	A risk assessment is conducted on an annual basis to identify potential threats, assess their significance, and document mitigation strategies adopted by the organization. The risk assessment considers factors including changes related to technology, environment, key vendors and business partners, and fraud.	Inquired of the Senior DevOps Engineer about the risk assessment process noting that a risk assessment was conducted on an annual basis to identify potential threats, assess their significance, and document mitigation strategies adopted by the organization. Also noted that the risk assessment considered factors including changes related to technology, environment, key vendors and business partners, and fraud. Inspected the most recent annual risk assessment noting that a risk assessment was conducted on an annual basis to identify potential threats, assess their significance, and document mitigation strategies adopted by the organization. Also noted that the risk assessment considered factors including changes related to technology, environment, key vendors and business partners, and fraud.	No exceptions noted. No exceptions noted.
		An independent Board of Directors oversees risks to Securly and meets on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and General Data Protection Regulation (GDPR).	Inquired of the Director of Engineering about the Board of Directors noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR. Inspected Board meeting minutes noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR.	No exceptions noted. No exceptions noted.

CC 2.0 Communication and Information				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Securly performs internal penetration testing on an annual basis. Any identified critical or high-risk findings are prioritized and tracked to completion.	Inquired of the Senior DevOps Engineer about the annual penetration test noting that Securly performed internal penetration testing on an annual basis. Noted that any identified critical or high-risk findings were prioritized and tracked to completion. Inspected the most recent penetration test results noting that Securly performed internal penetration testing on an annual basis. Also noted that there were no identified critical or high-risk findings during the examination period.	No exceptions noted. No exceptions noted.

CC 2.0 Communication and Information				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	A description of the system and changes to the system are made available to internal and external users via Securly's support portal. This description delineates the boundaries of the system and key aspects of processing, including user commitments and responsibilities.	Inquired of the Senior DevOps Engineer about the system description noting that a description of the system and changes to the system were made available to internal and external users via Securly's support portal. Also noted that this description delineated the boundaries of the system and key aspects of processing, including user commitments and responsibilities. Inspected the Securly support portal noting that a description of the system and changes to the system were made available to internal and external users via Securly's support portal. Also noted that this description delineated the boundaries of the system and key aspects of processing, including user commitments and responsibilities.	No exceptions noted. No exceptions noted.
		Written security, availability, and confidentiality policies addressing responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system have been approved by management, implemented throughout the company, and published on Google Drive and Confluence Wiki.	Inquired of the Senior DevOps Engineer about Securly's policies noting that written security, availability, and confidentiality policies addressing responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system had been approved by management, implemented throughout the company, and published on Google Drive and Confluence Wiki. Inspected Securly's policies and their location on Google Drive and Confluence Wiki noting that written security, availability, and confidentiality policies addressing responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system had been approved by management, implemented throughout the company, and published on Google Drive and Confluence Wiki.	No exceptions noted. No exceptions noted.

CC 2.0 Communication and Information				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		The Information Security Policy posted on Google Drive specifies which roles have authority and responsibilities over aspects of the system. In addition, the policy covers integrity and ethics. The Information Security Policy is reviewed and updated on an annual basis.	Inquired of the Senior DevOps Engineer about the Information Security Policy noting that the Information Security Policy posted on Google Drive specified which roles had authority and responsibilities over aspects of the system. Noted that the policy covered integrity and ethics. Also noted that the Information Security Policy was reviewed and updated on an annual basis. Inspected the Information Security Policy and its location on Google Drive noting that the Information Security Policy posted on Google Drive specified which roles had authority and responsibilities over aspects of the system. Noted that the policy covered integrity and ethics. Also noted that the Information Security Policy was reviewed and updated on an annual basis.	No exceptions noted. No exceptions noted.
		A Software Development Policy is in place to direct change management practices.	Inquired of the Senior DevOps Engineer about software development policies and procedures noting that a Software Development Policy was in place to direct change management practices. Inspected the Software Development Policy noting that the policy directed change management practices. Also noted that the policy defined the change management processes for normal and emergency changes.	No exceptions noted. No exceptions noted.
		Securly has a Data Classification and Handling Policy that defines confidential information.	Inquired of the Senior DevOps Engineer about the Data Classification and Handling Policy noting that Securly had a Data Classification and Handling Policy within the Information Security Policy that defined confidential information. Inspected the Data Classification and Handling Policy noting that Securly had a Data Classification and Handling Policy within the Information Security Policy that defined confidential information.	No exceptions noted. No exceptions noted.

CC 2.0 Communication and Information				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		A documented data disposal policy is in place within the Data Classification and Handling Policy.	Inquired of the Senior DevOps Engineer about disposal noting that a documented data disposal policy was in place within the Data Classification and Handling Policy. Inspected the Data Classification and Handling Policy noting that a documented data disposal policy was in place within the Data Classification and Handling Policy.	No exceptions noted. No exceptions noted.
		Management has communicated a description of its Privacy Policy on the company website.	Inquired of the Senior DevOps Engineer about the Privacy Policy noting that management had communicated a description of its Privacy Policy on the company website. Inspected the Privacy Policy and its location on the company website noting that management had communicated a description of its Privacy Policy on the company website.	No exceptions noted. No exceptions noted.
		System enhancements and releases are broadcasted to internal users via Slack.	Inquired of the Senior Build and Release Engineer: DevOps about release notes noting that system enhancements and releases were broadcasted to internal users via Slack. Inspected the Slack notifications for randomly selected system enhancements and application code changes during the examination period noting that system enhancements and releases were broadcasted to internal users via Slack.	No exceptions noted. No exceptions noted.

CC 2.0 Communication and Information				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	A description of the system and changes to the system are made available to internal and external users via Securly's support portal. This description delineates the boundaries of the system and key aspects of processing, including user commitments and responsibilities.	Inquired of the Senior DevOps Engineer about the system description noting that a description of the system and changes to the system were made available to internal and external users via Securly's support portal. Also noted that this description delineated the boundaries of the system and key aspects of processing, including user commitments and responsibilities. Inspected the Securly support portal noting that a description of the system and changes to the system were made available to internal and external users via Securly's support portal. Also noted that this description delineated the boundaries of the system and key aspects of processing, including user commitments and responsibilities.	No exceptions noted. No exceptions noted.
		For customers, a description of the system is discussed and provided as part of the Master Services Agreement (MSA), which also outlines the roles and responsibilities of the customer.	Inquired of the Senior DevOps Engineer about MSAs noting that for customers, a description of the system was discussed and provided as part of the MSA, which also outlined the roles and responsibilities of the customer. Inspected the MSA template and an executed MSA noting that for customers, a description of the system was discussed and provided as part of the MSA, which also outlined the roles and responsibilities of the customer.	No exceptions noted. No exceptions noted.
		Management has communicated a description of its Privacy Policy on the company website.	Inquired of the Senior DevOps Engineer about the Privacy Policy noting that management had communicated a description of its Privacy Policy on the company website. Inspected the Privacy Policy and its location on the company website noting that management had communicated a description of its Privacy Policy on the company website.	No exceptions noted. No exceptions noted.

CC 2.0 Communication and Information				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Third parties with access to confidential information have an executed agreement with Securly that includes requirements related to confidential information.	Inquired of the Director of Engineering about third party agreements noting that third parties with access to confidential information had a signed agreement with Securly that included requirements related to confidential information. Inspected the executed agreement with Amazon Web Services (third party with access to confidential information) noting that third parties with access to confidential information had an executed agreement with Securly that included requirements related to confidential information.	No exceptions noted. No exceptions noted.
		System enhancements and release notes are available for external users.	Inquired of the Senior Build and Release Engineer: DevOps about release notes noting that system enhancements and release notes were available for external users. Inspected the Securly support portal noting that system enhancements and release notes were available for external users.	No exceptions noted. No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	A risk assessment is conducted on an annual basis to identify potential threats, assess their significance, and document mitigation strategies adopted by the organization. The risk assessment considers factors including changes related to technology, environment, key vendors and business partners, and fraud.	Inquired of the Senior DevOps Engineer about the risk assessment process noting that a risk assessment was conducted on an annual basis to identify potential threats, assess their significance, and document mitigation strategies adopted by the organization. Also noted that the risk assessment considered factors including changes related to technology, environment, key vendors and business partners, and fraud. Inspected the most recent annual risk assessment noting that a risk assessment was conducted on an annual basis to identify potential threats, assess their significance, and document mitigation strategies adopted by the organization. Also noted that the risk assessment considered factors including changes related to technology, environment, key vendors and business partners, and fraud.	No exceptions noted. No exceptions noted.
		Agreements with new vendors and business partners are evaluated by management for associated risk prior to being implemented.	Inquired of the Senior DevOps Engineer about vendor and partner risk evaluations noting that agreements with new vendors and business partners were evaluated by management for associated risk prior to being implemented. Inspected the New Vendor Assessment form for new vendors during the examination period noting that management evaluated the company for associated risks prior to being implemented.	No exceptions noted. No exceptions noted.
		Securly performs internal penetration testing on an annual basis. Any identified critical or high-risk findings are prioritized and tracked to completion.	Inquired of the Senior DevOps Engineer about the annual penetration test noting that Securly performed internal penetration testing on an annual basis. Noted that any identified critical or high-risk findings were prioritized and tracked to completion. Inspected the most recent penetration test results noting that Securly performed internal penetration testing on an annual basis. Also noted that there were no identified critical or high-risk findings during the examination period.	No exceptions noted. No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Management reviews the SOC reports for Amazon Web Services, Elastic Cloud, and Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impact Securly's risk management strategy.	Inquired of the Senior DevOps Engineer about assessing subservice providers noting that management reviewed the SOC reports for Amazon Web Services, Elastic Cloud, and Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Amazon Web Services (AWS) SOC 2 Type 2 reports covering the periods of October 1, 2020 to March 31, 2021, and April 1, 2021 to September 30, 2021, the bridge letter, and management's review of the SOC report noting that management reviewed the SOC report for AWS to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Elastic Cloud SOC 2 Type 2 report covering the period of October 1, 2020 to October 31, 2021, the bridge letter, and management's review of the SOC report noting that management reviewed the SOC reports for Elastic Cloud to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Google Workspace SOC 2 Type 2 report covering the period November 1, 2020 to October 31, 2021, and management's review of the SOC report noting that management reviewed the SOC reports for Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		An independent Board of Directors oversees risks to Securly and meets on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and General Data Protection Regulation (GDPR).	Inquired of the Director of Engineering about the Board of Directors noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR. Inspected Board meeting minutes noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR.	No exceptions noted. No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	A risk assessment is conducted on an annual basis to identify potential threats, assess their significance, and document mitigation strategies adopted by the organization. The risk assessment considers factors including changes related to technology, environment, key vendors and business partners, and fraud.	Inquired of the Senior DevOps Engineer about the risk assessment process noting that a risk assessment was conducted on an annual basis to identify potential threats, assess their significance, and document mitigation strategies adopted by the organization. Also noted that the risk assessment considered factors including changes related to technology, environment, key vendors and business partners, and fraud. Inspected the most recent annual risk assessment noting that a risk assessment was conducted on an annual basis to identify potential threats, assess their significance, and document mitigation strategies adopted by the organization. Also noted that the risk assessment considered factors including changes related to technology, environment, key vendors and business partners, and fraud.	No exceptions noted. No exceptions noted.
		Agreements with new vendors and business partners are evaluated by management for associated risk prior to being implemented.	Inquired of the Senior DevOps Engineer about vendor and partner risk evaluations noting that agreements with new vendors and business partners were evaluated by management for associated risk prior to being implemented. Inspected the New Vendor Assessment form for new vendors during the examination period noting that management evaluated the company for associated risks prior to being implemented.	No exceptions noted. No exceptions noted.
		Securly performs internal penetration testing on an annual basis. Any identified critical or high-risk findings are prioritized and tracked to completion.	Inquired of the Senior DevOps Engineer about the annual penetration test noting that Securly performed internal penetration testing on an annual basis. Noted that any identified critical or high-risk findings were prioritized and tracked to completion. Inspected the most recent penetration test results noting that Securly performed internal penetration testing on an annual basis. Also noted that there were no identified critical or high-risk findings during the examination period.	No exceptions noted. No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Management reviews the SOC reports for Amazon Web Services, Elastic Cloud, and Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impact Securly's risk management strategy.	Inquired of the Senior DevOps Engineer about assessing subservice providers noting that management reviewed the SOC reports for Amazon Web Services, Elastic Cloud, and Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Amazon Web Services (AWS) SOC 2 Type 2 reports covering the periods of October 1, 2020 to March 31, 2021, and April 1, 2021 to September 30, 2021, the bridge letter, and management's review of the SOC report noting that management reviewed the SOC report for AWS to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Elastic Cloud SOC 2 Type 2 report covering the period of October 1, 2020 to October 31, 2021, the bridge letter, and management's review of the SOC report noting that management reviewed the SOC reports for Elastic Cloud to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Google Workspace SOC 2 Type 2 report covering the period November 1, 2020 to October 31, 2021, and management's review of the SOC report noting that management reviewed the SOC reports for Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		An independent Board of Directors oversees risks to Securly and meets on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and General Data Protection Regulation (GDPR).	Inquired of the Director of Engineering about the Board of Directors noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR. Inspected Board meeting minutes noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR.	No exceptions noted. No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	A risk assessment is conducted on an annual basis to identify potential threats, assess their significance, and document mitigation strategies adopted by the organization. The risk assessment considers factors including changes related to technology, environment, key vendors and business partners, and fraud.	Inquired of the Senior DevOps Engineer about the risk assessment process noting that a risk assessment was conducted on an annual basis to identify potential threats, assess their significance, and document mitigation strategies adopted by the organization. Also noted that the risk assessment considered factors including changes related to technology, environment, key vendors and business partners, and fraud. Inspected the most recent annual risk assessment noting that a risk assessment was conducted on an annual basis to identify potential threats, assess their significance, and document mitigation strategies adopted by the organization. Also noted that the risk assessment considered factors including changes related to technology, environment, key vendors and business partners, and fraud.	No exceptions noted. No exceptions noted.
		An independent Board of Directors oversees risks to Securly and meets on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and General Data Protection Regulation (GDPR).	Inquired of the Director of Engineering about the Board of Directors noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR. Inspected Board meeting minutes noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR.	No exceptions noted. No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	A risk assessment is conducted on an annual basis to identify potential threats, assess their significance, and document mitigation strategies adopted by the organization. The risk assessment considers factors including changes related to technology, environment, key vendors and business partners, and fraud.	Inquired of the Senior DevOps Engineer about the risk assessment process noting that a risk assessment was conducted on an annual basis to identify potential threats, assess their significance, and document mitigation strategies adopted by the organization. Also noted that the risk assessment considered factors including changes related to technology, environment, key vendors and business partners, and fraud. Inspected the most recent annual risk assessment noting that a risk assessment was conducted on an annual basis to identify potential threats, assess their significance, and document mitigation strategies adopted by the organization. Also noted that the risk assessment considered factors including changes related to technology, environment, key vendors and business partners, and fraud.	No exceptions noted. No exceptions noted.
		Agreements with new vendors and business partners are evaluated by management for associated risk prior to being implemented.	Inquired of the Senior DevOps Engineer about vendor and partner risk evaluations noting that agreements with new vendors and business partners were evaluated by management for associated risk prior to being implemented. Inspected the New Vendor Assessment form for new vendors during the examination period noting that management evaluated the company for associated risks prior to being implemented.	No exceptions noted. No exceptions noted.
		Securly performs internal penetration testing on an annual basis. Any identified critical or high-risk findings are prioritized and tracked to completion.	Inquired of the Senior DevOps Engineer about the annual penetration test noting that Securly performed internal penetration testing on an annual basis. Noted that any identified critical or high-risk findings were prioritized and tracked to completion. Inspected the most recent penetration test results noting that Securly performed internal penetration testing on an annual basis. Also noted that there were no identified critical or high-risk findings during the examination period.	No exceptions noted. No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Management reviews the SOC reports for Amazon Web Services, Elastic Cloud, and Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impact Securly's risk management strategy.	Inquired of the Senior DevOps Engineer about assessing subservice providers noting that management reviewed the SOC reports for Amazon Web Services, Elastic Cloud, and Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Amazon Web Services (AWS) SOC 2 Type 2 reports covering the periods of October 1, 2020 to March 31, 2021, and April 1, 2021 to September 30, 2021, the bridge letter, and management's review of the SOC report noting that management reviewed the SOC report for AWS to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Elastic Cloud SOC 2 Type 2 report covering the period of October 1, 2020 to October 31, 2021, the bridge letter, and management's review of the SOC report noting that management reviewed the SOC reports for Elastic Cloud to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Google Workspace SOC 2 Type 2 report covering the period November 1, 2020 to October 31, 2021, and management's review of the SOC report noting that management reviewed the SOC reports for Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		An independent Board of Directors oversees risks to Securly and meets on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and General Data Protection Regulation (GDPR).	Inquired of the Director of Engineering about the Board of Directors noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR. Inspected Board meeting minutes noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR.	No exceptions noted. No exceptions noted.

CC 4.0 Monitoring Activities				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Securly uses CloudWatch and VividCortex to monitor the network, servers, and measure availability, status, and performance.	Inquired of the DevOps Manager about network and server monitoring noting that Securly used CloudWatch and VividCortex to monitor the network, servers, and measure availability, status, and performance. Inspected the CloudWatch and VividCortex configurations noting that Securly used CloudWatch and VividCortex to monitor the network, servers, and measure availability, status, and performance.	No exceptions noted. No exceptions noted.
		AWS CloudWatch is used to monitor server network connections. CloudWatch and other tools are used to identify, log, and report potential security incidents. The system notifies IT via Slack of potential incidents in progress.	Inquired of the Senior DevOps Engineer about AWS CloudWatch noting that AWS CloudWatch was used to monitor server network connections. Noted that CloudWatch and other tools were used to identify, log, and report potential security incidents. Also noted that the system notified IT via Slack of potential incidents in progress. Inspected the AWS CloudWatch configurations and an example alert noting that AWS CloudWatch was used to monitor server network connections. Noted that CloudWatch and other tools were used to identify, log, and report potential security incidents. Also noted that the system notified IT via Slack of potential incidents in progress.	No exceptions noted. No exceptions noted.
		AWS CloudTrail sends alerts to identify potential security threats and changes to production, including security group changes on production account.	Inquired of the Senior DevOps Engineer about AWS CloudTrail noting that AWS CloudTrail sent alerts to identify potential security threats and changes to production, including security group changes on production account. Inspected CloudTrail configurations and an example alert noting that AWS CloudTrail sent alerts to identify potential security threats and changes to production, including security group changes on production account.	No exceptions noted. No exceptions noted.

CC 4.0 Monitoring Activities				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Securly uses AWS Config and CloudTrail to ensure compliance with security standards. The DevOps team is notified by email if the configuration becomes out of compliance with configured policies and issues are remediated.	Inquired of the Senior DevOps Engineer about security related notifications noting that Securly used AWS Config and CloudTrail to ensure compliance with security standards. Also noted that the DevOps team was notified by email if the configuration became out of compliance with configured policies and issues were remediated. Inspected the AWS CloudTrail configurations, the AWS Config rules, and an example alert noting that Securly used AWS Config and CloudTrail to ensure compliance with security standards. Also noted that the DevOps team was notified by email if configuration became out of compliance with configured policies and issues were remediated.	No exceptions noted. No exceptions noted.
		All production access to AWS and any changes made by an individual in AWS Console are logged using AWS CloudTrail.	Inquired of the Senior DevOps Engineer about CloudTrail noting that all production access to AWS and any changes made by an individual in AWS Console were logged using AWS CloudTrail. Inspected the AWS CloudTrail configurations and logs noting that production access to AWS and any changes made by an individual in AWS Console were logged using AWS CloudTrail.	No exceptions noted. No exceptions noted.
		Securly performs internal penetration testing on an annual basis. Any identified critical or high-risk findings are prioritized and tracked to completion.	Inquired of the Senior DevOps Engineer about the annual penetration test noting that Securly performed internal penetration testing on an annual basis. Noted that any identified critical or high-risk findings were prioritized and tracked to completion. Inspected the most recent penetration test results noting that Securly performed internal penetration testing on an annual basis. Also noted that there were no identified critical or high-risk findings during the examination period.	No exceptions noted. No exceptions noted.

CC 4.0 Monitoring Activities				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Internally and externally reported failures, security incidents, and concerns are documented and tracked until resolution by the Support team.	Inquired of the Senior DevOps Engineer about reported incidents noting that internally and externally reported failures, security incidents, and concerns were documented and tracked until resolution by the Support team. Inspected the ticket details for randomly selected internally and externally reported failures, security incidents, and concerns from the ticketing system during the examination period noting that the reported failures, security incidents, and concerns were documented and tracked until resolution by the Support team.	No exceptions noted. No exceptions noted.
		An independent Board of Directors oversees risks to Securly and meets on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and General Data Protection Regulation (GDPR).	Inquired of the Director of Engineering about the Board of Directors noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR. Inspected Board meeting minutes noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR.	No exceptions noted. No exceptions noted.

CC 5.0 Control Activities				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	A risk assessment is conducted on an annual basis to identify potential threats, assess their significance, and document mitigation strategies adopted by the organization. The risk assessment considers factors including changes related to technology, environment, key vendors and business partners, and fraud.	Inquired of the Senior DevOps Engineer about the risk assessment process noting that a risk assessment was conducted on an annual basis to identify potential threats, assess their significance, and document mitigation strategies adopted by the organization. Also noted that the risk assessment considered factors including changes related to technology, environment, key vendors and business partners, and fraud. Inspected the most recent annual risk assessment noting that a risk assessment was conducted on an annual basis to identify potential threats, assess their significance, and document mitigation strategies adopted by the organization. Also noted that the risk assessment considered factors including changes related to technology, environment, key vendors and business partners, and fraud.	No exceptions noted. No exceptions noted.
		Agreements with new vendors and business partners are evaluated by management for associated risk prior to being implemented.	Inquired of the Senior DevOps Engineer about vendor and partner risk evaluations noting that agreements with new vendors and business partners were evaluated by management for associated risk prior to being implemented. Inspected the New Vendor Assessment form for new vendors during the examination period noting that management evaluated the company for associated risks prior to being implemented.	No exceptions noted. No exceptions noted.
		Securly performs internal penetration testing on an annual basis. Any identified critical or high-risk findings are prioritized and tracked to completion.	Inquired of the Senior DevOps Engineer about the annual penetration test noting that Securly performed internal penetration testing on an annual basis. Noted that any identified critical or high-risk findings were prioritized and tracked to completion. Inspected the most recent penetration test results noting that Securly performed internal penetration testing on an annual basis. Also noted that there were no identified critical or high-risk findings during the examination period.	No exceptions noted. No exceptions noted.

CC 5.0 Control Activities				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Management reviews the SOC reports for Amazon Web Services, Elastic Cloud, and Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impact Securly's risk management strategy.	Inquired of the Senior DevOps Engineer about assessing subservice providers noting that management reviewed the SOC reports for Amazon Web Services, Elastic Cloud, and Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Amazon Web Services (AWS) SOC 2 Type 2 reports covering the periods of October 1, 2020 to March 31, 2021, and April 1, 2021 to September 30, 2021, the bridge letter, and management's review of the SOC report noting that management reviewed the SOC report for AWS to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Elastic Cloud SOC 2 Type 2 report covering the period of October 1, 2020 to October 31, 2021, the bridge letter, and management's review of the SOC report noting that management reviewed the SOC reports for Elastic Cloud to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Google Workspace SOC 2 Type 2 report covering the period November 1, 2020 to October 31, 2021, and management's review of the SOC report noting that management reviewed the SOC reports for Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.

CC 5.0 Control Activities				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		An independent Board of Directors oversees risks to Securly and meets on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and General Data Protection Regulation (GDPR).	Inquired of the Director of Engineering about the Board of Directors noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR. Inspected Board meeting minutes noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR.	No exceptions noted. No exceptions noted.

CC 5.0 Control Activities				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Agreements with new vendors and business partners are evaluated by management for associated risk prior to being implemented.	Inquired of the Senior DevOps Engineer about vendor and partner risk evaluations noting that agreements with new vendors and business partners were evaluated by management for associated risk prior to being implemented. Inspected the New Vendor Assessment form for new vendors during the examination period noting that management evaluated the company for associated risks prior to being implemented.	No exceptions noted. No exceptions noted.
		Securly performs internal penetration testing on an annual basis. Any identified critical or high-risk findings are prioritized and tracked to completion.	Inquired of the Senior DevOps Engineer about the annual penetration test noting that Securly performed internal penetration testing on an annual basis. Noted that any identified critical or high-risk findings were prioritized and tracked to completion. Inspected the most recent penetration test results noting that Securly performed internal penetration testing on an annual basis. Also noted that there were no identified critical or high-risk findings during the examination period.	No exceptions noted. No exceptions noted.

CC 5.0 Control Activities				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Management reviews the SOC reports for Amazon Web Services, Elastic Cloud, and Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impact Securly's risk management strategy.	Inquired of the Senior DevOps Engineer about assessing subservice providers noting that management reviewed the SOC reports for Amazon Web Services, Elastic Cloud, and Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Amazon Web Services (AWS) SOC 2 Type 2 reports covering the periods of October 1, 2020 to March 31, 2021, and April 1, 2021 to September 30, 2021, the bridge letter, and management's review of the SOC report noting that management reviewed the SOC report for AWS to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Elastic Cloud SOC 2 Type 2 report covering the period of October 1, 2020 to October 31, 2021, the bridge letter, and management's review of the SOC report noting that management reviewed the SOC reports for Elastic Cloud to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Google Workspace SOC 2 Type 2 report covering the period November 1, 2020 to October 31, 2021, and management's review of the SOC report noting that management reviewed the SOC reports for Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.

CC 5.0 Control Activities				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		An independent Board of Directors oversees risks to Securly and meets on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and General Data Protection Regulation (GDPR).	Inquired of the Director of Engineering about the Board of Directors noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR. Inspected Board meeting minutes noting that an independent Board of Directors oversaw risks to Securly and met on an annual basis to review the company's performance, operations, internal controls and any related deficiencies, and GDPR.	No exceptions noted. No exceptions noted.

CC 5.0 Control Activities				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Roles and responsibilities related to security are defined in written job descriptions.	Inquired of the IT Specialist about job descriptions noting that roles and responsibilities related to security were defined in written job descriptions. Inspected the job descriptions for randomly selected new employees during the examination period noting that roles and responsibilities related to security were defined in written job descriptions.	No exceptions noted. No exceptions noted.
		Written security, availability, and confidentiality policies addressing responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system have been approved by management, implemented throughout the company, and published on Google Drive and Confluence Wiki.	Inquired of the Senior DevOps Engineer about Securly's policies noting that written security, availability, and confidentiality policies addressing responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system had been approved by management, implemented throughout the company, and published on Google Drive and Confluence Wiki. Inspected Securly's policies and their location on Google Drive and Confluence Wiki noting that written security, availability, and confidentiality policies addressing responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system had been approved by management, implemented throughout the company, and published on Google Drive and Confluence Wiki.	No exceptions noted. No exceptions noted.

CC 5.0 Control Activities				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		The Information Security Policy posted on Google Drive specifies which roles have authority and responsibilities over aspects of the system. In addition, the policy covers integrity and ethics. The Information Security Policy is reviewed and updated on an annual basis.	Inquired of the Senior DevOps Engineer about the Information Security Policy noting that the Information Security Policy posted on Google Drive specified which roles had authority and responsibilities over aspects of the system. Noted that the policy covered integrity and ethics. Also noted that the Information Security Policy was reviewed and updated on an annual basis. Inspected the Information Security Policy and its location on Google Drive noting that the Information Security Policy posted on Google Drive specified which roles had authority and responsibilities over aspects of the system. Noted that the policy covered integrity and ethics. Also noted that the Information Security Policy was reviewed and updated on an annual basis.	No exceptions noted. No exceptions noted.
		Securly's employees and contractors are required to complete online Information Security Training on an annual basis. Topics include security, compliance, data leakage, technology trends, and acknowledgement of the Information Security Policy.	Inquired of the IT Specialist about security training noting that Securly's employees and contractors were required to complete online Information Security Training on an annual basis. Also noted that topics included security, compliance, data leakage, technology trends, and acknowledgement of the Information Security Policy. Inspected the Information Security Training documentation noting that topics included security, compliance, data leakage, technology trends, and acknowledgement of the Information Security Policy. Inspected the Information Security Training certificate and Information Security Policy acknowledgement for randomly selected current employees and contractors during the examination period noting that Securly's employees and contractors were required to complete online Information Security Training on an annual basis and acknowledge the Information Security Policy.	No exceptions noted. No exceptions noted. No exceptions noted.

CC 5.0 Control Activities				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		A Software Development Policy is in place to direct change management practices.	Inquired of the Senior DevOps Engineer about software development policies and procedures noting that a Software Development Policy was in place to direct change management practices. Inspected the Software Development Policy noting that the policy directed change management practices. Also noted that the policy defined the change management processes for normal and emergency changes.	No exceptions noted. No exceptions noted.
		Securly has a Data Classification and Handling Policy that defines confidential information.	Inquired of the Senior DevOps Engineer about the Data Classification and Handling Policy noting that Securly had a Data Classification and Handling Policy within the Information Security Policy that defined confidential information. Inspected the Data Classification and Handling Policy noting that Securly had a Data Classification and Handling Policy within the Information Security Policy that defined confidential information.	No exceptions noted. No exceptions noted.
		A documented data disposal policy is in place within the Data Classification and Handling Policy.	Inquired of the Senior DevOps Engineer about disposal noting that a documented data disposal policy was in place within the Data Classification and Handling Policy. Inspected the Data Classification and Handling Policy noting that a documented data disposal policy was in place within the Data Classification and Handling Policy.	No exceptions noted. No exceptions noted.
		Management has communicated a description of its Privacy Policy on the company website.	Inquired of the Senior DevOps Engineer about the Privacy Policy noting that management had communicated a description of its Privacy Policy on the company website. Inspected the Privacy Policy and its location on the company website noting that management had communicated a description of its Privacy Policy on the company website.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Internal users have write access to production using a unique user ID and password. There are no shared accounts in use that have write access. There are shared accounts for selected read-only users.	Inquired of the Director of Engineering about unique accounts noting that internal users had write access to production using a unique user ID and password. Noted that there were no shared accounts in use that had write access. Also noted that there were shared accounts for selected read-only users.	No exceptions noted.
			Inspected the AWS Identity and Access Management user listing, groups and its permissions noting that internal users had write access to production using a unique user ID and password. Noted that there were no shared accounts in use that had write access. Also noted that there were shared accounts for selected read-only users.	No exceptions noted.
		Securly password settings must be a minimum of eight characters and include complexity. Lockout occurs after three invalid attempts when technically feasible.	Inquired of the Senior DevOps Engineer about password settings noting that Securly password settings were a minimum of eight characters and included complexity. Also noted that lockout occurred after three invalid attempts when technically feasible.	No exceptions noted.
			Inspected the AWS IAM password configurations noting that Securly password settings were a minimum of eight characters and included complexity. Noted that lockout was not user configurable. Also noted that AWS was configured to enforce two-factor authentication.	No exceptions noted.
			Inspected the Google Workspace password configurations noting that Securly password settings were a minimum of eight characters, included complexity, and that lockout occurred after three invalid attempts when technically feasible.	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Securly has established baseline configuration standards for AWS. This includes requirements for restricted access, configuration standards, and standardized access control lists.	Inquired of the Senior DevOps Engineer about AWS baseline configurations noting that Securly had established baseline configuration standards for AWS. Also noted that this included requirements for restricted access, configuration standards, and standardized access control lists. Inspected baseline configuration standards noting that Securly had established baseline configuration standards for AWS. Also noted that this included requirements for restricted access, configuration standards, and standardized access control lists.	No exceptions noted. No exceptions noted.
		Network segmentation is in place for each application.	Inquired of the Senior DevOps Engineer about network segmentation noting that network segmentation was in place for each application. Inspected the non-production and production environments noting that the network was segregated for each application.	No exceptions noted. No exceptions noted.
		Access is implemented via single sign on (SSO) through Google authentication services or Microsoft Azure for external users.	Inquired of the Senior DevOps Engineer about customer access noting that access was implemented via SSO through Google authentication services or Microsoft Azure for external users. Inspected the SSO access implementation noting that access was implemented via SSO through Google authentication services or Microsoft Azure for external users.	No exceptions noted. No exceptions noted.
		Remote access to the production systems require logging into AWS Session Manager.	Inquired of the Director of Engineering about remote access noting that remote access to the production systems required logging into AWS Session Manager. Inspected the Session Manager configurations noting that remote access to the production system was encrypted and required logging into the AWS Session Manager.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Securly employs AWS Security Groups to protect cloud infrastructure resources of the differing production environments.	Inquired of the Senior DevOps Engineer about production security noting that Securly employed AWS Security Groups to protect cloud infrastructure resources of the differing production environments. Inspected AWS Security Group configurations noting that Securly employed AWS Security Groups to protect cloud infrastructure resources of the differing production environments.	No exceptions noted. No exceptions noted.
		Write access into the server and database level is restricted to the DevOps team, Director of Engineering, and DevOps Manager for the production environment.	Inquired of the Senior DevOps Engineer about system administrator access noting that write access into the server and database level was restricted to the DevOps team, Director of Engineering, and DevOps Manager for the production environment. Inspected the AWS Identity and Access Management administrative user listing including group memberships and respective permissions noting that write access into the server and database level was restricted to the DevOps team, Director of Engineering, and DevOps Manager for the production environment.	No exceptions noted. No exceptions noted.
		Role-based access to the system and its technology stack is approved by the System Administrator.	Inquired of the Director of Engineering about approvals for system and technology stack access noting that role-based access to the system and its technology stack must be approved by the System Administrator. Inspected the ticket documentation for randomly selected new employees during the examination period noting that role-based access to the system and its technology stack was approved by the System Administrator. Inspected the ticket documentation for randomly selected new contractors during the examination period noting that role-based access to the system and its technology stack was approved by the System Administrator.	No exceptions noted. No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Administrative access to AWS Console is restricted to members of the DevOps management and DevOps team.	Inquired of the Senior DevOps Engineer about admin permissions to AWS Console noting that administrative access to AWS Console was restricted to members of the DevOps management and DevOps team. Inspected AWS group memberships for groups with administrative access to the AWS Console noting that administrative access to the AWS Console was restricted to members of the DevOps management and DevOps team.	No exceptions noted. No exceptions noted.
		Access to AWS requires two-factor authentication.	Inquired of the Senior DevOps Engineer about AWS access noting that access to the AWS, which had all servers and databases, required two-factor authentication. Observed the AWS sign-in process noting that access to AWS required two-factor authentication. Inspected the AWS Identity and Access Management user access listing noting that each user was required to sign in with two-factor authentication to access AWS.	No exceptions noted. No exceptions noted. No exceptions noted.
		Access to the code repository is restricted and appropriateness of access to the repository is reviewed on a semi-annual basis.	Inquired of the Director of Engineering about repository access noting that access to the code repository was restricted, and appropriateness of access was reviewed by management on a semi-annual basis. Inspected the GitHub user listing and ticket documentation for the semi-annual GitHub user access reviews done during the examination period noting that appropriateness of access to the code repository was reviewed by management on a semi-annual basis.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Only the Build and Release team can update the main branch in GitHub and release software to production.	Inquired of the Director of Engineering about GitHub permissions noting that only the Build and Release team could update the main branch in GitHub and release software to production. Inspected the GitHub commit history, the GitHub administrator listing, the GitHub administrator permissions, and the Jenkins administrator listing noting that only the Build and Release team could update the main branch in GitHub and release software to production.	No exceptions noted. No exceptions noted.
		Access to migrate code to production is restricted to authorized personnel who do not have development or testing responsibilities.	Inquired of the Director of Engineering about code migration noting that access to migrate code to production was restricted to authorized personnel who did not have development or testing responsibilities. Inspected the GitHub user access listing and the Jenkins user access listing noting that none of the members with privileges to migrate code to production have development or testing responsibilities.	No exceptions noted. No exceptions noted.
		Only DevOps team members can release changes into the production environment.	Inquired of the Director of Engineering about Jenkins permissions noting that only DevOps team members could release changes into the production environment. Inspected the Jenkins administrative user access listing noting that only DevOps team members could release changes into the production environment.	No exceptions noted. No exceptions noted.
		Only DevOps and the Director of Engineering run and deploy configuration changes.	Inquired of the Director of Engineering about configuration changes noting that only DevOps and the Director of Engineering ran and deployed configuration changes. Inspected the AWS Identity and Access Management administrative user listing, groups and its permissions noting that only the DevOps team and the Director of Engineering had privileged access to run and deploy configuration changes.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Support personnel have specific change access to the database in order to make client configuration changes.	Inquired of the Director of Engineering about database permissions noting that support personnel had specific change access to the database in order to make client configuration changes. Inspected the support tool configuration and log noting that designated customer service accounts had privileges to make specific configuration changes. Also noted that the audit log recorded configuration changes made by the support personnel.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	New employee or contractor access is requested through an access request form or a ticket that is approved by Human Resources (HR) Management or other relevant system owners.	Inquired of the IT Specialist about access provisioning noting that new employee or contractor access was requested through an access request form or ticket that was approved by the HR Management or other relevant system owners.	No exceptions noted.
			Inspected the access request form or ticket documentation for randomly selected new employees during the examination period noting that new employee access was requested through an access request form or a ticket that was approved by HR Management or other relevant system owners.	No exceptions noted.
			Inspected the access request form or ticket documentation for randomly selected new contractors during the examination period noting that new contractor access was requested through an access request form or a ticket that was approved by HR Management or other relevant system owners.	No exceptions noted.
		Modified employee/contractor access is requested through the ticketing system and approved by the system owner.	Inquired of the IT Specialist about access changes noting that modified employee or contractor access was requested through the ticketing system and approved by the system owner. Also noted that there was only one access modification for employees and contractors during the examination period.	No exceptions noted.
			Inspected the ticket documentation for the access modification during the examination period noting that modification of access was requested through the ticketing system and approved by the system owner.	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Employee and contractor access to Securly's system and infrastructure systems is removed upon termination.	Inquired of the IT Specialist about access removal noting that employee and contractor access to Securly's system and infrastructure systems was removed upon termination. Inspected the ticket documentation and account details for randomly selected terminated employees and contractors during the examination period noting that access to Securly's system and infrastructure systems was removed upon termination.	No exceptions noted. No exceptions noted.
		The Securly system requires customers to identify an administrative account to self-manage their users.	Inquired of the Director of Engineering about Securly administrative access noting the Securly system required customers to identify an administrative account to self-manage their users. Observed a user act as a delegated customer service account administrator noting that the Securly system required customers to identify an administrative account to self-manage their users. Inspected the listing of administrators within the client table in the production database noting that each customer account had a designated administrator with the ability to self-manage their users.	No exceptions noted. No exceptions noted. No exceptions noted.
		User access reviews are performed on an annual basis. Unauthorized access is documented and remediated by management.	Inquired of the Director of Engineering about user access reviews noting that user access reviews were performed on an annual basis. Also noted that unauthorized access was documented and remediated by management. Inspected documentation of user access reviews during the examination period noting that user access reviews were performed on an annual basis. Also noted that unauthorized access was documented and remediated by management.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	New employee or contractor access is requested through an access request form or a ticket that is approved by Human Resources (HR) Management or other relevant system owners.	Inquired of the IT Specialist about access provisioning noting that new employee or contractor access was requested through an access request form or ticket that was approved by the HR Management or other relevant system owners.	No exceptions noted.
			Inspected the access request form or ticket documentation for randomly selected new employees during the examination period noting that new employee access was requested through an access request form or a ticket that was approved by HR Management or other relevant system owners.	No exceptions noted.
			Inspected the access request form or ticket documentation for randomly selected new contractors during the examination period noting that new contractor access was requested through an access request form or a ticket that was approved by HR Management or other relevant system owners.	No exceptions noted.
		Modified employee/contractor access is requested through the ticketing system and approved by the system owner.	Inquired of the IT Specialist about access changes noting that modified employee or contractor access was requested through the ticketing system and approved by the system owner. Also noted that there was only one access modification for employees and contractors during the examination period.	No exceptions noted.
			Inspected the ticket documentation for the access modification during the examination period noting that modification of access was requested through the ticketing system and approved by the system owner.	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Employee and contractor access to Securly's system and infrastructure systems is removed upon termination.	Inquired of the IT Specialist about access removal noting that employee and contractor access to Securly's system and infrastructure systems was removed upon termination. Inspected the ticket documentation and account details for randomly selected terminated employees and contractors during the examination period noting that access to Securly's system and infrastructure systems was removed upon termination.	No exceptions noted. No exceptions noted.
		The Securly system requires customers to identify an administrative account to self-manage their users.	Inquired of the Director of Engineering about Securly administrative access noting the Securly system required customers to identify an administrative account to self-manage their users. Observed a user act as a delegated customer service account administrator noting that the Securly system required customers to identify an administrative account to self-manage their users. Inspected the listing of administrators within the client table in the production database noting that each customer account had a designated administrator with the ability to self-manage their users.	No exceptions noted. No exceptions noted. No exceptions noted.
		User access reviews are performed on an annual basis. Unauthorized access is documented and remediated by management.	Inquired of the Director of Engineering about user access reviews noting that user access reviews were performed on an annual basis. Also noted that unauthorized access was documented and remediated by management. Inspected documentation of user access reviews during the examination period noting that user access reviews were performed on an annual basis. Also noted that unauthorized access was documented and remediated by management.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Management reviews the SOC reports for Amazon Web Services, Elastic Cloud, and Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impact Securly's risk management strategy.	Inquired of the Senior DevOps Engineer about assessing subservice providers noting that management reviewed the SOC reports for Amazon Web Services, Elastic Cloud, and Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Amazon Web Services (AWS) SOC 2 Type 2 reports covering the periods of October 1, 2020 to March 31, 2021, and April 1, 2021 to September 30, 2021, the bridge letter, and management's review of the SOC report noting that management reviewed the SOC report for AWS to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Elastic Cloud SOC 2 Type 2 report covering the period of October 1, 2020 to October 31, 2021, the bridge letter, and management's review of the SOC report noting that management reviewed the SOC reports for Elastic Cloud to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Google Workspace SOC 2 Type 2 report covering the period November 1, 2020 to October 31, 2021, and management's review of the SOC report noting that management reviewed the SOC reports for Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Employee and contractor access to Securly's system and infrastructure systems is removed upon termination.	Inquired of the IT Specialist about access removal noting that employee and contractor access to Securly's system and infrastructure systems was removed upon termination. Inspected the ticket documentation and account details for randomly selected terminated employees and contractors during the examination period noting that access to Securly's system and infrastructure systems was removed upon termination.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Management reviews the SOC reports for Amazon Web Services, Elastic Cloud, and Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impact Securly's risk management strategy.	Inquired of the Senior DevOps Engineer about assessing subservice providers noting that management reviewed the SOC reports for Amazon Web Services, Elastic Cloud, and Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Amazon Web Services (AWS) SOC 2 Type 2 reports covering the periods of October 1, 2020 to March 31, 2021, and April 1, 2021 to September 30, 2021, the bridge letter, and management's review of the SOC report noting that management reviewed the SOC report for AWS to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Elastic Cloud SOC 2 Type 2 report covering the period of October 1, 2020 to October 31, 2021, the bridge letter, and management's review of the SOC report noting that management reviewed the SOC reports for Elastic Cloud to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Google Workspace SOC 2 Type 2 report covering the period November 1, 2020 to October 31, 2021, and management's review of the SOC report noting that management reviewed the SOC reports for Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		A documented data disposal policy is in place within the Data Classification and Handling Policy.	Inquired of the Senior DevOps Engineer about disposal noting that a documented data disposal policy was in place within the Data Classification and Handling Policy. Inspected the Data Classification and Handling Policy noting that a documented data disposal policy was in place within the Data Classification and Handling Policy.	No exceptions noted. No exceptions noted.
		Securly deletes customer data within 60 days of a submitted customer request.	Inquired of the Director of Engineering about data retention noting that Securly deleted customer data within 60 days of a submitted customer request. Also noted that there were no customer data deletion requests during the examination period. Inspected the Data Classification and Handling Policy noting that the policy stated Securly deleted customer data within 60 days of a submitted customer request.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Securly uses CloudWatch and VividCortex to monitor the network, servers, and measure availability, status, and performance.	Inquired of the DevOps Manager about network and server monitoring noting that Securly used CloudWatch and VividCortex to monitor the network, servers, and measure availability, status, and performance. Inspected the CloudWatch and VividCortex configurations noting that Securly used CloudWatch and VividCortex to monitor the network, servers, and measure availability, status, and performance.	No exceptions noted. No exceptions noted.
		AWS CloudWatch is used to monitor server network connections. CloudWatch and other tools are used to identify, log, and report potential security incidents. The system notifies IT via Slack of potential incidents in progress.	Inquired of the Senior DevOps Engineer about AWS CloudWatch noting that AWS CloudWatch was used to monitor server network connections. Noted that CloudWatch and other tools were used to identify, log, and report potential security incidents. Also noted that the system notified IT via Slack of potential incidents in progress. Inspected the AWS CloudWatch configurations and an example alert noting that AWS CloudWatch was used to monitor server network connections. Noted that CloudWatch and other tools were used to identify, log, and report potential security incidents. Also noted that the system notified IT via Slack of potential incidents in progress.	No exceptions noted. No exceptions noted.
		The ability to make changes to the AWS environment is restricted to the DevOps team, Senior Vice President (SVP) and Director of Engineering.	Inquired of the Senior DevOps Engineer about AWS access permissions noting that the ability to make changes to the AWS environment was restricted to the DevOps team, SVP and Director of Engineering. Inspected the AWS Identity and Access Management user listing noting that the ability to make changes to the AWS environment was restricted to the DevOps team, SVP and Director of Engineering.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Access to AWS requires two-factor authentication.	Inquired of the Senior DevOps Engineer about AWS access noting that access to the AWS, which had all servers and databases, required two-factor authentication. Observed the AWS sign-in process noting that access to AWS required two-factor authentication. Inspected the AWS Identity and Access Management user access listing noting that each user was required to sign in with two-factor authentication to access AWS.	No exceptions noted. No exceptions noted. No exceptions noted.
		Access to the code repository is restricted and appropriateness of access to the repository is reviewed on a semi-annual basis.	Inquired of the Director of Engineering about repository access noting that access to the code repository was restricted, and appropriateness of access was reviewed by management on a semi-annual basis. Inspected the GitHub user listing and ticket documentation for the semi-annual GitHub user access reviews done during the examination period noting that appropriateness of access to the code repository was reviewed by management on a semi-annual basis.	No exceptions noted. No exceptions noted.
		Remote access to the production systems require logging into AWS Session Manager.	Inquired of the Director of Engineering about remote access noting that remote access to the production systems required logging into AWS Session Manager. Inspected the Session Manager configurations noting that remote access to the production system was encrypted and required logging into the AWS Session Manager.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Securly employs AWS Security Groups to protect cloud infrastructure resources of the differing production environments.	Inquired of the Senior DevOps Engineer about production security noting that Securly employed AWS Security Groups to protect cloud infrastructure resources of the differing production environments. Inspected AWS Security Group configurations noting that Securly employed AWS Security Groups to protect cloud infrastructure resources of the differing production environments.	No exceptions noted. No exceptions noted.
		Domain Name System (DNS) requests are only accepted from authenticated users.	Inquired of the Senior DevOps Engineer about DNS requests noting that DNS requests were only accepted from authenticated users. Inspected the DNS proxy configurations noting that DNS requests were only accepted from authenticated users.	No exceptions noted. No exceptions noted.
		Applications, except Auditor, run over HTTPS.	Inquired of the Senior DevOps Engineer about end user access noting that applications, except Auditor, ran over HTTPS. Inspected the HTTPS encryption certificate and configurations noting that applications, except Auditor, ran over HTTPS.	No exceptions noted. No exceptions noted.
		Linux servers are behind AWS Security Groups to prevent malicious file uploads.	Inquired of the Senior DevOps Engineer about server security noting that Linux servers were behind AWS Security Groups to prevent malicious file uploads. Inspected the AWS Security Groups that contained the Securly Linux servers and the inbound ruleset noting that Linux servers were assigned to an AWS Security Group to prevent malicious file uploads.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Elastic Cloud is used to encrypt data at rest.	Inquired of the Senior DevOps Engineer about encryption noting that Elastic Cloud was used to encrypt data at rest. Inspected the Elastic Cloud SOC 2 Type 2 report noting that Elastic Cloud was used to encrypt data at rest.	No exceptions noted. No exceptions noted.
		Auditor only services Simple Mail Transfer Protocol (SMTP) requests from whitelisted domains.	Inquired of the Principal DevOps Manager about Auditor noting that Auditor only serviced SMTP requests from whitelisted domains. Inspected the whitelisted domains code and the list of whitelisted domains noting that Auditor only serviced SMTP requests from whitelisted domains.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Securly employs AWS Security Groups to protect cloud infrastructure resources of the differing production environments.	Inquired of the Senior DevOps Engineer about production security noting that Securly employed AWS Security Groups to protect cloud infrastructure resources of the differing production environments. Inspected AWS Security Group configurations noting that Securly employed AWS Security Groups to protect cloud infrastructure resources of the differing production environments.	No exceptions noted. No exceptions noted.
		Domain Name System (DNS) requests are only accepted from authenticated users.	Inquired of the Senior DevOps Engineer about DNS requests noting that DNS requests were only accepted from authenticated users. Inspected the DNS proxy configurations noting that DNS requests were only accepted from authenticated users.	No exceptions noted. No exceptions noted.
		Applications, except Auditor, run over HTTPS.	Inquired of the Senior DevOps Engineer about end user access noting that applications, except Auditor, ran over HTTPS. Inspected the HTTPS encryption certificate and configurations noting that applications, except Auditor, ran over HTTPS.	No exceptions noted. No exceptions noted.
		Linux servers are behind AWS Security Groups to prevent malicious file uploads.	Inquired of the Senior DevOps Engineer about server security noting that Linux servers were behind AWS Security Groups to prevent malicious file uploads. Inspected the AWS Security Groups that contained the Securly Linux servers and the inbound ruleset noting that Linux servers were assigned to an AWS Security Group to prevent malicious file uploads.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Patch management procedures are in place for key system components.	Inquired of the Senior DevOps Engineer about patching noting that patch management procedures were in place for key system components.	No exceptions noted.
			Inspected the Patching and Vulnerability Management policy noting that patch management procedures were in place for key system components.	No exceptions noted.
			Inspected the change ticket details for randomly selected system enhancement and application code changes, which included application and software patches, during the examination period noting that each change went through the formal change control process that required testing and management approval.	No exceptions noted.
			Inspected change ticket details for randomly selected emergency changes, which included emergency application and software patches, from the ticketing system during the examination period noting that emergency changes to production systems went through the formal change control process that required testing and management approval.	No exceptions noted.
		A documented data disposal policy is in place within the Data Classification and Handling Policy.	Inquired of the Senior DevOps Engineer about disposal noting that a documented data disposal policy was in place within the Data Classification and Handling Policy.	No exceptions noted.
			Inspected the Data Classification and Handling Policy noting that a documented data disposal policy was in place within the Data Classification and Handling Policy.	No exceptions noted.
		Auditor only services Simple Mail Transfer Protocol (SMTP) requests from whitelisted domains.	Inquired of the Principal DevOps Manager about Auditor noting that Auditor only serviced SMTP requests from whitelisted domains.	No exceptions noted.
			Inspected the whitelisted domains code and the list of whitelisted domains noting that Auditor only serviced SMTP requests from whitelisted domains.	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Access to the code repository is restricted and appropriateness of access to the repository is reviewed on a semi-annual basis.	Inquired of the Director of Engineering about repository access noting that access to the code repository was restricted, and appropriateness of access was reviewed by management on a semi-annual basis. Inspected the GitHub user listing and ticket documentation for the semi-annual GitHub user access reviews done during the examination period noting that appropriateness of access to the code repository was reviewed by management on a semi-annual basis.	No exceptions noted. No exceptions noted.
		Access to migrate code to production is restricted to authorized personnel who do not have development or testing responsibilities.	Inquired of the Director of Engineering about code migration noting that access to migrate code to production was restricted to authorized personnel who did not have development or testing responsibilities. Inspected the GitHub user access listing and the Jenkins user access listing noting that none of the members with privileges to migrate code to production have development or testing responsibilities.	No exceptions noted. No exceptions noted.
		Only DevOps team members can release changes into the production environment.	Inquired of the Director of Engineering about Jenkins permissions noting that only DevOps team members could release changes into the production environment. Inspected the Jenkins administrative user access listing noting that only DevOps team members could release changes into the production environment.	No exceptions noted. No exceptions noted.
		Only DevOps and the Director of Engineering run and deploy configuration changes.	Inquired of the Director of Engineering about configuration changes noting that only DevOps and the Director of Engineering ran and deployed configuration changes. Inspected the AWS Identity and Access Management administrative user listing, groups and its permissions noting that only the DevOps team and the Director of Engineering had privileged access to run and deploy configuration changes.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Support personnel have specific change access to the database in order to make client configuration changes.	Inquired of the Director of Engineering about database permissions noting that support personnel had specific change access to the database in order to make client configuration changes.	No exceptions noted.
			Inspected the support tool configuration and log noting that designated customer service accounts had privileges to make specific configuration changes. Also noted that the audit log recorded configuration changes made by the support personnel.	No exceptions noted.
		Patch management procedures are in place for key system components.	Inquired of the Senior DevOps Engineer about patching noting that patch management procedures were in place for key system components.	No exceptions noted.
			Inspected the Patching and Vulnerability Management policy noting that patch management procedures were in place for key system components.	No exceptions noted.
			Inspected the change ticket details for randomly selected system enhancement and application code changes, which included application and software patches, during the examination period noting that each change went through the formal change control process that required testing and management approval.	No exceptions noted.
			Inspected change ticket details for randomly selected emergency changes, which included emergency application and software patches, from the ticketing system during the examination period noting that emergency changes to production systems went through the formal change control process that required testing and management approval.	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Securly uses CloudWatch and VividCortex to monitor the network, servers, and measure availability, status, and performance.	Inquired of the DevOps Manager about network and server monitoring noting that Securly used CloudWatch and VividCortex to monitor the network, servers, and measure availability, status, and performance. Inspected the CloudWatch and VividCortex configurations noting that Securly used CloudWatch and VividCortex to monitor the network, servers, and measure availability, status, and performance.	No exceptions noted. No exceptions noted.
		AWS CloudWatch is used to monitor server network connections. CloudWatch and other tools are used to identify, log, and report potential security incidents. The system notifies IT via Slack of potential incidents in progress.	Inquired of the Senior DevOps Engineer about AWS CloudWatch noting that AWS CloudWatch was used to monitor server network connections. Noted that CloudWatch and other tools were used to identify, log, and report potential security incidents. Also noted that the system notified IT via Slack of potential incidents in progress. Inspected the AWS CloudWatch configurations and an example alert noting that AWS CloudWatch was used to monitor server network connections. Noted that CloudWatch and other tools were used to identify, log, and report potential security incidents. Also noted that the system notified IT via Slack of potential incidents in progress.	No exceptions noted. No exceptions noted.
		AWS CloudTrail sends alerts to identify potential security threats and changes to production, including security group changes on production account.	Inquired of the Senior DevOps Engineer about AWS CloudTrail noting that AWS CloudTrail sent alerts to identify potential security threats and changes to production, including security group changes on production account. Inspected CloudTrail configurations and an example alert noting that AWS CloudTrail sent alerts to identify potential security threats and changes to production, including security group changes on production account.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Securly uses AWS Config and CloudTrail to ensure compliance with security standards. The DevOps team is notified by email if the configuration becomes out of compliance with configured policies and issues are remediated.	Inquired of the Senior DevOps Engineer about security related notifications noting that Securly used AWS Config and CloudTrail to ensure compliance with security standards. Also noted that the DevOps team was notified by email if the configuration became out of compliance with configured policies and issues were remediated. Inspected the AWS CloudTrail configurations, the AWS Config rules, and an example alert noting that Securly used AWS Config and CloudTrail to ensure compliance with security standards. Also noted that the DevOps team was notified by email if configuration became out of compliance with configured policies and issues were remediated.	No exceptions noted. No exceptions noted.
		All production access to AWS and any changes made by an individual in AWS Console are logged using AWS CloudTrail.	Inquired of the Senior DevOps Engineer about CloudTrail noting that all production access to AWS and any changes made by an individual in AWS Console were logged using AWS CloudTrail. Inspected the AWS CloudTrail configurations and logs noting that production access to AWS and any changes made by an individual in AWS Console were logged using AWS CloudTrail.	No exceptions noted. No exceptions noted.
		Securly performs internal penetration testing on an annual basis. Any identified critical or high-risk findings are prioritized and tracked to completion.	Inquired of the Senior DevOps Engineer about the annual penetration test noting that Securly performed internal penetration testing on an annual basis. Noted that any identified critical or high-risk findings were prioritized and tracked to completion. Inspected the most recent penetration test results noting that Securly performed internal penetration testing on an annual basis. Also noted that there were no identified critical or high-risk findings during the examination period.	No exceptions noted. No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Securly uses CloudWatch and VividCortex to monitor the network, servers, and measure availability, status, and performance.	Inquired of the DevOps Manager about network and server monitoring noting that Securly used CloudWatch and VividCortex to monitor the network, servers, and measure availability, status, and performance. Inspected the CloudWatch and VividCortex configurations noting that Securly used CloudWatch and VividCortex to monitor the network, servers, and measure availability, status, and performance.	No exceptions noted. No exceptions noted.
		AWS CloudWatch is used to monitor server network connections. CloudWatch and other tools are used to identify, log, and report potential security incidents. The system notifies IT via Slack of potential incidents in progress.	Inquired of the Senior DevOps Engineer about AWS CloudWatch noting that AWS CloudWatch was used to monitor server network connections. Noted that CloudWatch and other tools were used to identify, log, and report potential security incidents. Also noted that the system notified IT via Slack of potential incidents in progress. Inspected the AWS CloudWatch configurations and an example alert noting that AWS CloudWatch was used to monitor server network connections. Noted that CloudWatch and other tools were used to identify, log, and report potential security incidents. Also noted that the system notified IT via Slack of potential incidents in progress.	No exceptions noted. No exceptions noted.
		AWS CloudTrail sends alerts to identify potential security threats and changes to production, including security group changes on production account.	Inquired of the Senior DevOps Engineer about AWS CloudTrail noting that AWS CloudTrail sent alerts to identify potential security threats and changes to production, including security group changes on production account. Inspected CloudTrail configurations and an example alert noting that AWS CloudTrail sent alerts to identify potential security threats and changes to production, including security group changes on production account.	No exceptions noted. No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Securly uses AWS Config and CloudTrail to ensure compliance with security standards. The DevOps team is notified by email if the configuration becomes out of compliance with configured policies and issues are remediated.	Inquired of the Senior DevOps Engineer about security related notifications noting that Securly used AWS Config and CloudTrail to ensure compliance with security standards. Also noted that the DevOps team was notified by email if the configuration became out of compliance with configured policies and issues were remediated. Inspected the AWS CloudTrail configurations, the AWS Config rules, and an example alert noting that Securly used AWS Config and CloudTrail to ensure compliance with security standards. Also noted that the DevOps team was notified by email if configuration became out of compliance with configured policies and issues were remediated.	No exceptions noted. No exceptions noted.
		All production access to AWS and any changes made by an individual in AWS Console are logged using AWS CloudTrail.	Inquired of the Senior DevOps Engineer about CloudTrail noting that all production access to AWS and any changes made by an individual in AWS Console were logged using AWS CloudTrail. Inspected the AWS CloudTrail configurations and logs noting that production access to AWS and any changes made by an individual in AWS Console were logged using AWS CloudTrail.	No exceptions noted. No exceptions noted.
		Securly performs internal penetration testing on an annual basis. Any identified critical or high-risk findings are prioritized and tracked to completion.	Inquired of the Senior DevOps Engineer about the annual penetration test noting that Securly performed internal penetration testing on an annual basis. Noted that any identified critical or high-risk findings were prioritized and tracked to completion. Inspected the most recent penetration test results noting that Securly performed internal penetration testing on an annual basis. Also noted that there were no identified critical or high-risk findings during the examination period.	No exceptions noted. No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Securly performs internal penetration testing on an annual basis. Any identified critical or high-risk findings are prioritized and tracked to completion.	Inquired of the Senior DevOps Engineer about the annual penetration test noting that Securly performed internal penetration testing on an annual basis. Noted that any identified critical or high-risk findings were prioritized and tracked to completion. Inspected the most recent penetration test results noting that Securly performed internal penetration testing on an annual basis. Also noted that there were no identified critical or high-risk findings during the examination period.	No exceptions noted. No exceptions noted.
		Incident response policies and procedures, which include the responsibility and process for reporting operational failures, security incidents, system problems, concerns, and user complaints, are published and available to internal users via Confluence Wiki.	Inquired of the Senior DevOps Engineer about incidents noting that incident response policies and procedures, which included the responsibility and process for reporting operational failures, security incidents, system problems, concerns, and user complaints, were published and available to internal users via Confluence Wiki. Inspected incident response policies and procedures and their location on the Confluence Wiki noting that incident response policies and procedures, which included the responsibility and process for reporting operational failures, security incidents, system problems, concerns, and user complaints, were published and available to internal users via Confluence Wiki.	No exceptions noted. No exceptions noted.
		Internally and externally reported failures, security incidents, and concerns are documented and tracked until resolution by the Support team.	Inquired of the Senior DevOps Engineer about reported incidents noting that internally and externally reported failures, security incidents, and concerns were documented and tracked until resolution by the Support team. Inspected the ticket details for randomly selected internally and externally reported failures, security incidents, and concerns from the ticketing system during the examination period noting that the reported failures, security incidents, and concerns were documented and tracked until resolution by the Support team.	No exceptions noted. No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Incident response policies and procedures, which include the responsibility and process for reporting operational failures, security incidents, system problems, concerns, and user complaints, are published and available to internal users via Confluence Wiki.	Inquired of the Senior DevOps Engineer about incidents noting that incident response policies and procedures, which included the responsibility and process for reporting operational failures, security incidents, system problems, concerns, and user complaints, were published and available to internal users via Confluence Wiki. Inspected incident response policies and procedures and their location on the Confluence Wiki noting that incident response policies and procedures, which included the responsibility and process for reporting operational failures, security incidents, system problems, concerns, and user complaints, were published and available to internal users via Confluence Wiki.	No exceptions noted. No exceptions noted.
		External users use the website support portal to report technical issues, concerns, and incidents.	Inquired of the Senior DevOps Engineer about client support noting that external users used the website support portal to report technical issues, concerns, and incidents. Inspected the client support portal noting that external users used the website support portal to report technical issues, concerns, and incidents.	No exceptions noted. No exceptions noted.
		Internally and externally reported failures, security incidents, and concerns are documented and tracked until resolution by the Support team.	Inquired of the Senior DevOps Engineer about reported incidents noting that internally and externally reported failures, security incidents, and concerns were documented and tracked until resolution by the Support team. Inspected the ticket details for randomly selected internally and externally reported failures, security incidents, and concerns from the ticketing system during the examination period noting that the reported failures, security incidents, and concerns were documented and tracked until resolution by the Support team.	No exceptions noted. No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Incident response policies and procedures, which include the responsibility and process for reporting operational failures, security incidents, system problems, concerns, and user complaints, are published and available to internal users via Confluence Wiki.	Inquired of the Senior DevOps Engineer about incidents noting that incident response policies and procedures, which included the responsibility and process for reporting operational failures, security incidents, system problems, concerns, and user complaints, were published and available to internal users via Confluence Wiki. Inspected incident response policies and procedures and their location on the Confluence Wiki noting that incident response policies and procedures, which included the responsibility and process for reporting operational failures, security incidents, system problems, concerns, and user complaints, were published and available to internal users via Confluence Wiki.	No exceptions noted. No exceptions noted.
		External users use the website support portal to report technical issues, concerns, and incidents.	Inquired of the Senior DevOps Engineer about client support noting that external users used the website support portal to report technical issues, concerns, and incidents. Inspected the client support portal noting that external users used the website support portal to report technical issues, concerns, and incidents.	No exceptions noted. No exceptions noted.
		Internally and externally reported failures, security incidents, and concerns are documented and tracked until resolution by the Support team.	Inquired of the Senior DevOps Engineer about reported incidents noting that internally and externally reported failures, security incidents, and concerns were documented and tracked until resolution by the Support team. Inspected the ticket details for randomly selected internally and externally reported failures, security incidents, and concerns from the ticketing system during the examination period noting that the reported failures, security incidents, and concerns were documented and tracked until resolution by the Support team.	No exceptions noted. No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Incident response policies and procedures, which include the responsibility and process for reporting operational failures, security incidents, system problems, concerns, and user complaints, are published and available to internal users via Confluence Wiki.	Inquired of the Senior DevOps Engineer about incidents noting that incident response policies and procedures, which included the responsibility and process for reporting operational failures, security incidents, system problems, concerns, and user complaints, were published and available to internal users via Confluence Wiki. Inspected incident response policies and procedures and their location on the Confluence Wiki noting that incident response policies and procedures, which included the responsibility and process for reporting operational failures, security incidents, system problems, concerns, and user complaints, were published and available to internal users via Confluence Wiki.	No exceptions noted. No exceptions noted.
		External users use the website support portal to report technical issues, concerns, and incidents.	Inquired of the Senior DevOps Engineer about client support noting that external users used the website support portal to report technical issues, concerns, and incidents. Inspected the client support portal noting that external users used the website support portal to report technical issues, concerns, and incidents.	No exceptions noted. No exceptions noted.
		Internally and externally reported failures, security incidents, and concerns are documented and tracked until resolution by the Support team.	Inquired of the Senior DevOps Engineer about reported incidents noting that internally and externally reported failures, security incidents, and concerns were documented and tracked until resolution by the Support team. Inspected the ticket details for randomly selected internally and externally reported failures, security incidents, and concerns from the ticketing system during the examination period noting that the reported failures, security incidents, and concerns were documented and tracked until resolution by the Support team.	No exceptions noted. No exceptions noted.

CC 8.0 Change Management				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	A Software Development Policy is in place to direct change management practices.	Inquired of the Senior DevOps Engineer about software development policies and procedures noting that a Software Development Policy was in place to direct change management practices. Inspected the Software Development Policy noting that the policy directed change management practices. Also noted that the policy defined the change management processes for normal and emergency changes.	No exceptions noted. No exceptions noted.
		GitHub is used to manage code and enforce version control, and Jira is used as the ticketing system.	Inquired of the Senior Build and Release Engineer (DevOps) about version control and tracking procedures noting that GitHub was used to manage code and enforce version control, and Jira was used as the ticketing system. Inspected the change ticket details and the version log for randomly selected system enhancement and application code changes during the examination period noting that each change was logged in the GitHub version log and had a corresponding Jira ticket to document the change management process.	No exceptions noted. No exceptions noted.
		Securly maintains separate development, test, and production environments.	Inquired of the Senior DevOps Engineer about environment segregation noting that Securly maintained separate development, test, and production environments. Inspected the development, test, and production environment hosts noting that Securly maintained separate development, test, and production environments.	No exceptions noted. No exceptions noted.

CC 8.0 Change Management				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Normal and emergency changes to production systems go through a formal change control process that requires testing and management approval.	Inquired of the DevOps Manager about change procedures noting that normal and emergency changes to production systems went through a formal change control process that required testing and management approval.	No exceptions noted.
			Inspected the Jira Workflow and Review Configuration noting that it defined the change control process for normal and emergency changes, which included testing and management approval.	No exceptions noted.
			Inspected the change ticket details for randomly selected system enhancement and application code changes (normal changes) during the examination period noting that each change went through a formal change control process that required testing and management approval.	No exceptions noted.
			Inspected change ticket details for randomly selected emergency changes, which included emergency application and software patches, from the ticketing system during the examination period noting that emergency changes to production systems went through the formal change control process that required testing and management approval.	No exceptions noted.
		Infrastructure changes are planned and documented.	Inquired of the DevOps Manager about infrastructure changes noting that infrastructure changes were planned and documented.	No exceptions noted.
			Inspected the change ticket details for randomly selected infrastructure changes during the examination period noting that infrastructure changes were planned and documented.	No exceptions noted.

CC 8.0 Change Management				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Changes are tested prior to release into the production environment.	Inquired of the Senior Build and Release Engineer (DevOps) about automated testing noting that changes were tested prior to release into the production environment. Inspected the change ticket details for randomly selected system enhancement and application code changes during the examination period noting that the change was tested prior to release into the production environment.	No exceptions noted. No exceptions noted.
		Releases are first placed in a QA environment where they are tested, and then placed in the beta environment. Only after confirming the releases are they deployed to the production environment.	Inquired of the Senior Build and Release Engineer (DevOps) about release migration noting that releases were first placed in a QA environment where they were tested, and then placed in the beta environment. Also noted that only after confirming the releases were they deployed to the production environment. Inspected the change ticket details for randomly selected system enhancement and application code changes during the examination period noting that each release was first placed in the QA environment for testing, and then placed in the beta environment. Also noted that the releases were deployed to production after management confirmed the releases in the beta environment.	No exceptions noted. No exceptions noted.

CC 8.0 Change Management				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Code must be reviewed by another Engineer prior to being released into the production environment.	Inquired of the Senior Build and Release Engineer (DevOps) about code review noting that code was reviewed by another Engineer prior to being released into the production environment. Inspected the Jira Workflow and Review Configurations noting that the ticketing system required changes to go through pull request reviews before merging the changes in preparation for deployment to the production environment. Inspected the change ticket details for randomly selected system enhancement and application code changes during the examination period noting that code was reviewed by another Engineer prior to being released into the production environment.	No exceptions noted. No exceptions noted. No exceptions noted.
		Only the Build and Release team can update the main branch in GitHub and release software to production.	Inquired of the Director of Engineering about GitHub permissions noting that only the Build and Release team could update the main branch in GitHub and release software to production. Inspected the GitHub commit history, the GitHub administrator listing, the GitHub administrator permissions, and the Jenkins administrator listing noting that only the Build and Release team could update the main branch in GitHub and release software to production.	No exceptions noted. No exceptions noted.
		Access to migrate code to production is restricted to authorized personnel who do not have development or testing responsibilities.	Inquired of the Director of Engineering about code migration noting that access to migrate code to production was restricted to authorized personnel who did not have development or testing responsibilities. Inspected the GitHub user access listing and the Jenkins user access listing noting that none of the members with privileges to migrate code to production have development or testing responsibilities.	No exceptions noted. No exceptions noted.

CC 8.0 Change Management				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Only DevOps team members can release changes into the production environment.	Inquired of the Director of Engineering about Jenkins permissions noting that only DevOps team members could release changes into the production environment. Inspected the Jenkins administrative user access listing noting that only DevOps team members could release changes into the production environment.	No exceptions noted. No exceptions noted.
		System enhancements and releases are broadcasted to internal users via Slack.	Inquired of the Senior Build and Release Engineer: DevOps about release notes noting that system enhancements and releases were broadcasted to internal users via Slack. Inspected the Slack notifications for randomly selected system enhancements and application code changes during the examination period noting that system enhancements and releases were broadcasted to internal users via Slack.	No exceptions noted. No exceptions noted.
		System enhancements and release notes are available for external users.	Inquired of the Senior Build and Release Engineer: DevOps about release notes noting that system enhancements and release notes were available for external users. Inspected the Securly support portal noting that system enhancements and release notes were available for external users.	No exceptions noted. No exceptions noted.

CC 9.0 Risk Mitigation				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from business disruption.	Securly has safe mode to ensure high availability during AWS or Securly infrastructure outages to avoid downtime.	Inquired of the Senior DevOps Engineer about system availability noting that Securly had safe mode to ensure high availability during AWS or Securly infrastructure outages to avoid downtime. Inspected the safe mode configuration, history log, and an example safe mode notification noting that Securly had safe mode to ensure high availability during AWS or Securly infrastructure outages to avoid downtime. Also noted that the safe mode tool automatically notified executive management and DevOps when safe mode was enabled.	No exceptions noted. No exceptions noted.
		Backup data is replicated to a data center for availability purposes via AWS.	Inquired of the Senior DevOps Engineer about backups noting that backup data was replicated to a data center in a different geographic location for availability purposes via AWS. Inspected the AWS instance configurations for availability zones noting that backup data was replicated to a data center for availability purposes via AWS.	No exceptions noted. No exceptions noted.
		Databases are backed up through daily snapshots.	Inquired of the DevOps Manager about database backups noting that databases were backed up through daily snapshots. Inspected snapshot configurations and snapshot logs for the production databases noting that the databases were backed up through daily snapshots.	No exceptions noted. No exceptions noted.
		Annual data restoration is performed to test the viability of backups.	Inquired of the DevOps Manager about data restoration noting that annual data restoration was performed to test the viability of backups. Inspected evidence of management's most recent annual data restoration test results noting that annual data restoration was performed to test the viability of backups.	No exceptions noted. No exceptions noted.

CC 9.0 Risk Mitigation				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Database backup procedures have been documented and are tested annually.	Inquired of the DevOps Manager about backup procedures noting that database backup procedures had been documented and were tested annually.	No exceptions noted.
			Inspected the Backup and Restoration Plan and Procedures document noting that database backup and restore procedures were documented. Also noted that the document established an annual cadence to test the production database backups.	No exceptions noted.
			Inspected evidence of management's most recent annual data restoration test results noting that annual data restoration was performed to test the viability of backups.	No exceptions noted.
		Securly maintains insurance coverage related to business continuity and cybersecurity threats.	Inquired of the Senior DevOps Engineer about insurance coverage noting that Securly maintained insurance coverage related to business continuity and cybersecurity threats.	No exceptions noted.
			Inspected the certificates of insurance provided from the insurers noting that Securly maintained insurance coverage related to business continuity and cybersecurity threats.	No exceptions noted.

CC 9.0 Risk Mitigation				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 9.2	The entity assesses and manages risks associated with vendors and business partners.	Agreements with new vendors and business partners are evaluated by management for associated risk prior to being implemented.	Inquired of the Senior DevOps Engineer about vendor and partner risk evaluations noting that agreements with new vendors and business partners were evaluated by management for associated risk prior to being implemented. Inspected the New Vendor Assessment form for new vendors during the examination period noting that management evaluated the company for associated risks prior to being implemented.	No exceptions noted. No exceptions noted.

CC 9.0 Risk Mitigation				
	Trust Services Criteria	**Controls Specified by Securly**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Management reviews the SOC reports for Amazon Web Services, Elastic Cloud, and Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impact Securly's risk management strategy.	Inquired of the Senior DevOps Engineer about assessing subservice providers noting that management reviewed the SOC reports for Amazon Web Services, Elastic Cloud, and Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Amazon Web Services (AWS) SOC 2 Type 2 reports covering the periods of October 1, 2020 to March 31, 2021, and April 1, 2021 to September 30, 2021, the bridge letter, and management's review of the SOC report noting that management reviewed the SOC report for AWS to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Elastic Cloud SOC 2 Type 2 report covering the period of October 1, 2020 to October 31, 2021, the bridge letter, and management's review of the SOC report noting that management reviewed the SOC reports for Elastic Cloud to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.
			Inspected the Google Workspace SOC 2 Type 2 report covering the period November 1, 2020 to October 31, 2021, and management's review of the SOC report noting that management reviewed the SOC reports for Google Workspace to assess potential risks, including security, availability, environmental, and technological changes which impacted Securly's risk management strategy.	No exceptions noted.

MOSSADAMS