

## New York

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: Erie 1 Board of Cooperative Educational Services (the “**Local Education Agency**” or “**LEA**” or “**New York Original LEA**”) and Rethink Autism, Inc. (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 documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in New York. Specifically, those are New York Education Law § 2-d; and the Regulations of the Commissioner of Education at 8 NYCRR Part 121; and

**WHEREAS**, the Parties wish to enter into these additional terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. Provider agrees to offer the LEA all the same terms and conditions found in the **MA-ME-NH-RI-VT-NDPA, Standard Version 1.0** Data Privacy Agreement between the Provider **Nashua School District** (Originating LEA”) which is dated **February 4, 2024** (“Originating DPA”). The terms and conditions of the Originating DPA are thus incorporated herein.
2. Provider additionally agrees to the following additional terms outlined in the attached Exhibit “G” for New York, which will control in the event of a conflict between the DPA and the Originating DPA.
3. Provider may, by signing the attached form of “General Offer of Privacy Terms” be bound by the terms of the General Offer of Privacy Terms to any other LEA who signs the acceptance on said Offer. The form is limited by the terms and conditions described therein.
4. **Notices**. All notices or other communication required or permitted to be given pursuant to the Originating DPA may be given for the LEA 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: Diana Frezza

Title: Chief Engagement Officer

Address: 49 W. 27th Street, 8th Floor, New York, NY 10001

Phone: 646-257-2919

Email: rfp@rethinked.com

The designated representative for the LEA for this DPA is:

Michelle Okal-Frink, Director of Instructional Technology, Research & Innovation  
355 Harlem Road, West Seneca, NY 14224  
(716) 821-7200 mokal@e1b.org

**Erie 1 Board of Cooperative Educational Services**

By: James Fregelette  
Date: Jun 3, 2025  
Printed Name: James Fregelette  
Title/Position: Executive Director

**Rethink Autism, Inc.**

By: Diana Frezza  
Date: 5/29/2025  
Printed Name: Diana Frezza  
Title/Position: Chief Engagement Officer

## **Exhibit "G"**

### **New York**

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the DPA.
3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA's Data Security and Privacy Policy. The LEA's Data Security Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security Policy to the Provider upon execution of Exhibit "E". Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations.
4. Provider represents that their Data Privacy and Security Plan can be found at the URL link listed in Exhibit K and is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a) implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the service agreement; (c) complies with the LEA's parents bill of rights for data privacy and security; (d) requires training of all providers' employees, assignees and subprocessors who have Access to student data or APPR data; (e) ensures subprocessors are required to protect PII received under this service agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, deletion and destruction.
5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit "E".
6. All references in the DPA to "Student Data" shall be amended to include and state, "Student Data and APPR Data."
7. To amend Article II, Section 5 to add: Provider shall ensure that its subprocessors agree that they do not have any property, licensing or ownership rights or claims to Student Data or APPR data and that they will comply with the LEA's Data Privacy and Security Policy. Provider shall examine the data privacy and security measures of its Subprocessors. If at any point a Subprocessor fails to materially comply with the requirements of this DPA, Provider shall: (i) notify LEA, (ii) as applicable, remove such Subprocessor's Access to Student Data and APPR Data; and (iii) as applicable, retrieve all Student Data and APPR Data received or stored by such Subprocessor and/or ensure that Student Data and APPR

Data has been securely deleted or securely destroyed in accordance with this DPA. In the event there is an incident in which Student Data and APPR Data held, possessed, or stored by the Subprocessor is compromised, or unlawfully Accessed or disclosed, Provider shall follow the Data Breach reporting requirements set forth in the DPA.

8. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
9. To amend Article IV, Section 3 to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data and APPR Data will be trained on the federal and state laws governing confidentiality of such Student Data and APPR Data prior to receipt. Access to or Disclosure of Student Data and APPR Data shall only be provided to Provider’s employees and subprocessors who need to know the Student Data and APPR Data to provide the services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide such services.
10. To replace Article IV, Section 6 (Disposition of Data) with the following: 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 ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider’s certifying that it and its subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any Assurance of Discontinuation, which will control in the case of a conflict.

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 ninety (90) days 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”**, or, with reasonable notice to the Provider, other form of its choosing. 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**”.

11. To amend Article IV, Section 7 to add: 'Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, "which term shall not include students."
12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
13. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an 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 or its designee(s) 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 or its designee(s) 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.

Upon request by the New York State Education Department's Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require Provider to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider's expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider's privacy and security practices that was issued no more than twelve months before the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the NIST Cybersecurity Framework v1.1 or any update to this Framework that is adopted by the New York State Department of Education.

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 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; and
  - vi. The number of records affected, if known; and
  - vii. A description of the investigation undertaken so far; and
  - viii. The name of a point of contact for Provider.
- (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. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals.
- (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.
- (6) Provider and its subprocessors will cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

15. To amend the definitions in Exhibit "C" as follows:

- "Subprocessor" is equivalent to subcontractor. It is a third party who the provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its service, and who has access to Student Data.
- "Provider" is also known as third party contractor. It any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to

such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

16. To add to Exhibit "C" the following definitions:

- **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting.
- **APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d
- **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration, including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.
- **Disclose or Disclosure:** The intentional or unintentional communication, release, or transfer of Student Data and/or APPR Data by any means, including oral, written, or electronic.
- **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
- **Release:** Shall have the same meaning as Disclose
- **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services, then the term LEA shall also include Participating School Districts for purposes of the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.
- **Participating School District:** As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement with LEA, and shall include LEA if it uses the Services in its own educational or operational programs.

-

**Exhibit “J”**

**LEA Documents**

LEA’s Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy, and supplemental information for this service agreement can be accessed at:

[https://sdpc.a4l.org/ny\\_dp\\_bor\\_url.php?districtID=13045](https://sdpc.a4l.org/ny_dp_bor_url.php?districtID=13045)



## **Exhibit “K”**

### **Provider Security Policy**

Provider’s Data Security and Privacy Plan can be accessed at:

Please see the attachments provided as well as our Privacy Policy at : <https://www.rethinked.com/privacy-policy/>

**STANDARD STUDENT DATA PRIVACY AGREEMENT**

**MASSACHUSETTS, MAINE, NEW HAMPSHIRE, RHODE ISLAND AND VERMONT**

**MA-ME-NH-RI-VT-NDPA, Standard Version 1.0**

**Nashua School District**

**and**

**Rethink Autism, Inc.**

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: Nashua School District, located at 141 Ledge Street, Nashua, NH 03060 USA (the “**Local Education Agency**” or “**LEA**”) and Rethink Autism, Inc., located at 49 West 27th Street, 8th Floor New York, NY 10001 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 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, 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. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
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: Diana Frezza \_\_\_\_\_ Title: EVP/GM \_\_\_\_\_

Address: 49 W. 27th Street, 8th Floor, New York, NY 10001 Phone: 646.257.2919

Email: rfp@rethinked.com \_\_\_\_\_

The designated representative for the LEA for this DPA is:

Greg Rodriguez, Director of Technology  
Nashua School District  
RodriguezG@nashua.edu  
141 Ledge Street, Nashua, NH 03060  
Phone: 603-966-1000

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

**Nashua School District**

By: Gregory Rodriguez  
Gregory Rodriguez (Apr 4, 2024 08:12 EDT)

Date: 04/04/24

Printed Name: Gregory Rodriguez

Title/Position: Director of Technology

**Rethink Autism, Inc.**

By: Diana Frezza

Date: 2/4/2024

Printed Name: Diana Frezza

Title/Position: EVP/GM

## **STANDARD CLAUSES**

Version 1.0

### **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.
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

## **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 in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. 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 the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. 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**

**RethinkEd**, web based resources that combine the power of technology and research to deliver evidence based tools, assessments and resources to support the whole child.

**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.	X
	Other application technology meta data-Please specify:	X
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	X
	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	X
Demographics	Date of Birth	X
	Place of Birth	
	Gender	X
	Ethnicity or race	X
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	
	Guidance counselor	X
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	X
	Phone	X
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	X

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

**[Insert Name of District or LEA]** Provider 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:

**[Insert categories of data here]**

\_\_\_\_\_ 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:

**[Insert or attach special instructions]**

3. Schedule of Disposition

Data shall be disposed of by the following date:

\_\_\_\_\_ As soon as commercially practicable.

\_\_\_\_\_ By **[Insert Date]**

4. Signature

\_\_\_\_\_  
Authorized Representative of LEA

\_\_\_\_\_  
Date

5. Verification of Disposition of Data

\_\_\_\_\_  
Authorized Representative of Company

\_\_\_\_\_  
Date

**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**

	<b>MAINTAINING ORGANIZATION/GROUP</b>	<b>FRAMEWORK(S)</b>
X	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
X	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
X	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
X	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”**  
**Massachusetts**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and Massachusetts General Law Chapter 93H; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Massachusetts;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Massachusetts does not require data to be stored within the United States.

## **EXHIBIT "G"**

### **Maine**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Maine. Specifically, those laws are 20-A M.R.S. §6001-6005.; 20-A M.R.S. §951 et. seq., Maine Unified Special Education Regulations, Maine Dep't of Edu. Rule Ch. 101; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Maine;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
4. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
5. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
6. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
7. The parties agree that the definition of Student Data in Exhibit "C" includes information that:
  - a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;
  - b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or
  - c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes.

**EXHIBIT “G”**  
**Rhode Island**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Rhode Island. Specifically, those laws are R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Rhode Island;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
4. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
5. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
6. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
  - i. Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact:
    1. The credit reporting agencies
    2. Remediation service providers
    3. The attorney general
  - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
  - iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student’s ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student’s requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

## **EXHIBIT “G”**

### **Vermont**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Vermont. Specifically, those laws are 9 VSA 2443 to 2443f; 16 VSA 1321 to 1324; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Vermont;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

**EXHIBIT "G"**  
**New Hampshire**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Hampshire;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. All references in the DPA to "Student Data" shall be amended to state "Student Data and Teacher Data." "Teacher Data" is defined as at least the following:

Social security number.  
Date of birth.  
Personal street address.  
Personal email address.  
Personal telephone number  
Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

"Teacher" means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "I"**.
3. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
4. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,..."
5. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
6. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes.

7. The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:
- (1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
  - (2) Limit unsuccessful logon attempts;
  - (3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
  - (4) Authorize wireless access prior to allowing such connections;
  - (5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
  - (6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;
  - (7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
  - (8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;
  - (9) Enforce a minimum password complexity and change of characters when new passwords are created;
  - (10) Perform maintenance on organizational systems;
  - (11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
  - (12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;
  - (13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;
  - (14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
  - (15) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;
  - (16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;



- (17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;
- (18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);
- (19) Protect the confidentiality of Student Data and Teacher Data at rest;
- (20) Identify, report, and correct system flaws in a timely manner;
- (21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;
- (22) Monitor system security alerts and advisories and take action in response; and
- (23) Update malicious code protection mechanisms when new releases are available.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

- 8. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
  - i. The estimated number of students and teachers affected by the breach, if any.
- 9. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.
- 10. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.

EXHIBIT "I" – TEACHER 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	
Communications	Online communications that are captured (emails, blog entries)	
Demographics	Date of Birth	
	Place of Birth	
	Social Security Number	
	Ethnicity or race	
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	
	Personal Email	
	Personal Phone	
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	
	Teacher calendar	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Teacher app username	
	Teacher app passwords	
Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
Teacher work	Teacher generated content; writing, pictures etc.	
	Other teacher work data -Please specify:	
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	







# RethinkEd\_Nashua\_5State\_VendorSigned

Final Audit Report

2024-04-04

Created:	2024-04-03
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAUm-sBQ5ZC_Rd5Zu17ph-V1ndfpOHS2jT

## "RethinkEd\_Nashua\_5State\_VendorSigned" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)  
2024-04-03 - 8:58:47 PM GMT- IP address: 108.35.203.7
-  Document emailed to rodriguezg@nashua.edu for signature  
2024-04-03 - 8:58:56 PM GMT
-  Email viewed by rodriguezg@nashua.edu  
2024-04-04 - 12:11:03 PM GMT- IP address: 3.80.89.126
-  Signer rodriguezg@nashua.edu entered name at signing as Gregory Rodriguez  
2024-04-04 - 12:12:05 PM GMT- IP address: 50.237.188.174
-  Document e-signed by Gregory Rodriguez (rodriguezg@nashua.edu)  
Signature Date: 2024-04-04 - 12:12:07 PM GMT - Time Source: server- IP address: 50.237.188.174
-  Agreement completed.  
2024-04-04 - 12:12:07 PM GMT



**RethinkFirst**

---

# Information Security Program

Last Updated: 8/19/2022

## Executive Summary

---

In recognition of the critical role that information systems play in Rethink Autism, Inc.'s business activities, this program defines the business rules and other requirements necessary for the secure and reliable operation of the information systems infrastructure of Rethink Autism, Inc. and all of its affiliates and business divisions.

This program defines baseline control measures that every Rethink employee is expected to be familiar with and to consistently follow. These security measures are the minimum required to prevent, among other things, customer data breaches and system unavailability. These policies also define the minimum controls necessary to prevent potential legal issues such as allegations of negligence or privacy violations. This document details both reasonable and practical ways for Rethink to prevent unnecessary losses.

Rethink critically depends on continued customer confidence. While trust is difficult to gain and can take years to achieve, it's even more difficult and costly to regain trust after it's been lost. The trust that customers have in Rethink should be considered a competitive advantage that must be nurtured and grown with efforts such as this information security program.

## Table of Contents

---

<b>EXECUTIVE SUMMARY .....</b>	<b>1</b>
<b>DOCUMENT CHANGE CONTROL .....</b>	<b>4</b>
<b>INFORMATION SECURITY TEAM.....</b>	<b>5</b>
<b>INCIDENT MANAGEMENT POLICY .....</b>	<b>5</b>
INCIDENT REPORT: .....	6
DOCUMENTATION .....	7
PERSONAL DATA BREACH PROCEDURE .....	8
<b>ACCEPTABLE USE POLICY .....</b>	<b>8</b>
COMPANY DEVICES.....	8
PERSONAL DEVICES .....	8
INFORMATION SECURITY.....	9
PASSWORD REQUIREMENTS .....	9
AUTHORIZED USE POLICY.....	9
INFORMATION SYSTEMS OWNERS .....	9
RISKS/LIABILITIES/DISCLAIMERS.....	10
SOFTWARE SECURITY .....	10
<b>CLOUD COMPUTING AND EXTERNAL SERVICES POLICY .....</b>	<b>12</b>
SCOPE.....	12
POLICY .....	12



<b>DATA RETENTION POLICY .....</b>	<b>13</b>
COMPANY DATA .....	13
RETENTION DURATION .....	13
<i>Rethink Business Records</i> .....	13
<i>Customer Administrative Records</i> .....	13
<i>Disposal</i> .....	13
<i>Customer Data</i> .....	14
<b>INFORMATION CLASSIFICATION POLICY .....</b>	<b>14</b>
ACCESS CONTROL .....	14
SYSTEM ACCESS CONTROLS .....	14
INFORMATION CLASSIFICATION .....	15
INFORMATION TRANSFER .....	16
<b>MEDIA PROTECTION AND DATA HANDLING POLICY .....</b>	<b>16</b>
PURPOSE .....	16
SCOPE .....	17
DEFINITIONS .....	17
GOVERNING LAWS AND REGULATIONS .....	17
POLICY STATEMENTS .....	18
<b>SECURITY AWARENESS TRAINING POLICY .....</b>	<b>19</b>
PURPOSE .....	19
SCOPE .....	19
DEFINITIONS .....	19
GOVERNING LAWS AND REGULATIONS .....	20
POLICY STATEMENTS .....	20
<b>SYSTEM CONFIGURATION MANAGEMENT POLICY .....</b>	<b>21</b>
PURPOSE .....	21
SCOPE .....	21
DEFINITIONS .....	21
GOVERNING LAWS AND REGULATIONS .....	21
POLICY STATEMENTS .....	22
<i>Basic Security Requirements:</i> .....	22
<i>Derived Security Requirements:</i> .....	22
<b>SYSTEM MAINTENANCE POLICY .....</b>	<b>23</b>
PURPOSE .....	23
SCOPE .....	23
DEFINITIONS .....	23
GOVERNING LAWS AND REGULATIONS .....	23
POLICY STATEMENTS .....	24
<b>VULNERABILITY MANAGEMENT AND SECURITY ASSESSMENT POLICY .....</b>	<b>25</b>
PURPOSE .....	25
SCOPE .....	25



DEFINITIONS.....	25
GOVERNING LAWS AND REGULATIONS .....	25
POLICY STATEMENTS.....	26
<b>CHANGE MANAGEMENT POLICY .....</b>	<b>26</b>
OVERVIEW .....	26
PURPOSE .....	26
SCOPE.....	27
DEFINITIONS AND ABBREVIATIONS.....	27
GOVERNING LAWS AND REGULATIONS .....	27
POLICY STATEMENTS.....	27
<b>SOFTWARE DEVELOPMENT LIFE CYCLE .....</b>	<b>31</b>
PURPOSE .....	31
SCOPE.....	31
DEFINITIONS.....	31
POLICY STATEMENTS.....	31
<b>WIRELESS SETUP AND ACCESS POLICY .....</b>	<b>33</b>
OVERVIEW .....	33
PURPOSE .....	33
SCOPE.....	33
POLICY .....	33
<i>Introduction .....</i>	<i>33</i>
<i>Connectivity Considerations.....</i>	<i>33</i>
<i>Security .....</i>	<i>34</i>
<i>Audit Controls and Management.....</i>	<i>34</i>
<b>BYOD POLICY .....</b>	<b>34</b>
OBJECTIVE .....	34
SCOPE.....	35
PROCEDURE .....	35
<i>Device protocols.....</i>	<i>35</i>
<i>Restrictions on authorized use .....</i>	<i>35</i>
<i>Privacy/company access .....</i>	<i>35</i>
<i>Safety .....</i>	<i>36</i>
<i>Lost, stolen, hacked or damaged equipment.....</i>	<i>36</i>
<b>LOST MEDIA OR LAPTOP .....</b>	<b>37</b>
<b>EARLY ACCESS POLICY .....</b>	<b>38</b>
OBJECTIVE .....	38
SCOPE.....	38
PROCEDURE .....	38
<b>RELEASE MANAGEMENT POLICY .....</b>	<b>38</b>
OVERVIEW .....	38
PURPOSE .....	38



STANDARD CHANGE PROCESS.....	39
HOTFIX CHANGE PROCESS.....	39
<b>FRONT END DEPENDENCY UPGRADE POLICY .....</b>	<b>39</b>
OVERVIEW AND SCOPE.....	39
RATIONALE .....	39
PROCESS.....	39
EXCLUSIONS AND FORKED PACKAGES .....	40
EXAMPLES .....	40
<b>EMPLOYEE ON-CALL POLICY.....</b>	<b>41</b>
OVERVIEW .....	41
ELIGIBILITY .....	41
SCHEDULE.....	41
GUIDELINES.....	41
ESCALATION .....	41
<b>BACKGROUND CHECK POLICY .....</b>	<b>42</b>
PURPOSE OF BACKGROUND CHECK:.....	42
POLICY: .....	42
RECORDKEEPING: .....	44
<b>LOG MANAGEMENT POLICY.....</b>	<b>44</b>
PURPOSE .....	44
SCOPE.....	44
POLICY .....	44
REVIEW POLICY.....	44
<b>RETHINK MEMBER ACKNOWLEDGEMENT.....</b>	<b>45</b>

## Document Change Control

Date	Version	Requester	Change/Review Notes
8/19/22	1.0	Stephen Churpakovich	Created and Consolidated IT Policies



## Information Security Team

Name	Group
Eran Rosenthal	President & COO
Amir Segev	CTO
Patty Mah	CFO
Stephen Churpakovich	Director of Information Security
Robert Johnson	General Counsel
Brandon Anderson	Director of Infrastructure
Maria Sakata	HR
Margarita Burakov	VP of Engineering
Brad Wilson	VP of Enterprise Architecture

Each individual is responsible for participating in security team meetings and disseminating information to his or her team. Additionally, each security team member is responsible for being aware of tools being introduced to their team and informing the Security Team Lead for audit.

## Incident Management Policy

This section discusses the steps taken in response to an incident that affects the security of information that Rethink processes (each, an “incident”). Such incidents may include system outages, data loss or theft.

The person who discovers the incident may be a Rethink staff member, or someone outside of Rethink. Regardless of the source, when the incident is known to a Rethink staff member, he or she must contact the Rethink Privacy Officer or, if the Rethink Privacy Officer is not available, the Head of Engineering should be contacted. The CEO should also be contacted if the incident includes a general failure of Rethink production systems.



The Rethink Privacy Officer or Head of Engineering will assemble a response team that may consist of any or all development or product personnel necessary to address the issue. Rethink utilizes several methods of team communication including phone, email, SMS, MS Teams, and Slack. All of these methods should be utilized until the proper individual is notified and a response is initiated.

## Incident Report:

Each Incident report will track the following information:

- The name of the initial reporter
- Time of the call
- Contact information about the caller, if external
- The nature of the incident
- The equipment or persons involved
- How the incident was detected
- When the event was first noticed that supported the idea that the incident occurred

The Rethink staff member who identifies the issue (or receives the report) will add the following:

- Is the equipment affected business critical?
- What is the severity of the potential impact?
- Name of system being targeted, along with operating system and IP address.
- Any information about the origin of the attack.
- Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy.
- Is the incident real or perceived?
- Is the incident still in progress?
- What data or property is threatened and how critical is it?
- What is the impact on the business should the attack succeed? Minimal, serious, or critical?
- What system or systems are targeted, where are they located physically and on the network?
- Is the incident inside the trusted network?
- Is the response urgent?
- Can the incident be quickly contained?
- Will the response alert the attacker and do we care?
- What type of incident is this? Example: virus, worm, intrusion, abuse, damage. An incident ticket will be created.

The incident will be categorized into the highest applicable level of one of the following categories:

- Category one - A threat to public safety or life.
- Category two - A threat to sensitive data
- Category three - A threat to computer systems
- Category four - A disruption of services

Team members will respond based on the incident assessment and proceed utilizing the Security Incident Response policy and procedure.



The response team may create additional procedures which are not foreseen in this document. If there is no applicable procedure in place, the team must document what was done and later establish a procedure for the incident. Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization. Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:

- Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
- Make users change passwords if passwords may have been sniffed.
- Be sure the system has been hardened by turning off or uninstalling unused services.
- Be sure the system is fully patched.
- Be sure real time virus protection and intrusion detection is running.
- Be sure the system is logging the correct events and to the proper level.

## Documentation

The following shall be documented:

- How the incident was discovered.
- The category of the incident.
- How the incident occurred, whether through email, firewall, etc.
- Where the attack came from, such as IP addresses and other related information about the attacker.
- What was done in response?
- Whether the response was effective.
- Evidence Preservation—make copies of logs, email, and other communication.
- Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.
- Notify proper external agencies—notify the police and other appropriate agencies if prosecution of the intruder is possible.
- Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.
- Review response and update policies—plan and take preventative steps so the intrusion can't happen again.
- Consider whether an additional policy could have prevented the intrusion.
- Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
- Was the incident response appropriate? How could it be improved?
- Was every appropriate party informed in a timely manner?
- Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?
- Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, antivirus updated, email policies set, etc.?
- Have changes been made to prevent a new and similar infection?



- Should any security policies be updated?
- What lessons have been learned from this experience?

Upon management approval, the changes will be implemented.

## Personal Data Breach Procedure

Not every incident that compromises information security is a data breach. In general, a data breach is defined by applicable law and triggers obligations to notify affected individuals and governmental authorities.

## Acceptable Use Policy

---

Rethink defines acceptable business use as activities that directly or indirectly support Rethink. Rethink defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.

## Company Devices

Rethink issues Personal Computers to all employees. Local storage of documents, company data, customer data and other similar information is not allowed by policy. Information classified as Highly Confidential and Confidential should be stored within Rethink's cloud-based services.

Company-issued devices may not be used at any time to:

- Store or transmit illicit materials
- Store or transmit proprietary information
- Harass others
- Engage in outside business activities

## Personal Devices

While occasional personal use of Company Technology is permitted, the usage must not violate Company policy or law and must not interfere with daily work.

Personal devices may access the Rethink wireless network when used for company business.

Connectivity issues with personal devices are not supported by Rethink; employees should contact the device manufacturer and/or their carrier for operating system or hardware-related issues. Log in to company accounts and systems through secure and private networks is required.

Employees may use personal devices to access company-controlled services with the following restrictions:

- Personal devices may not be used to store or access Highly Confidential or Confidential information.
- Personal devices may not be used to administer Rethink systems without prior approval by the Rethink Privacy Officer or CEO.



- Rethink recommends that personal devices must be password/passcode protected using the features of the device. In all cases, a strong password is required to access company online resources. Biometrics security features may also be approved by management and the Security Operations team.

## Information Security

Employee access to Rethink online resources is controlled via the software service provider. Employees' access to information is limited based on the Information Classification Policy. Employees are required to utilize best practices that are developed and implemented by Rethink, at all times. Conducting Rethink business that results in the storage and/or processing of sensitive data on non-Rethink controlled environments, including a Cloud Service Provider with which Rethink does not have a contractual agreement which covers the data stored with the Cloud Storage Provider, is prohibited.

## Password Requirements

Rethink's password requirements are:

- Passwords must be at least eight characters and a combination of upper- and lower-case letters, numbers, and symbols.
- Passwords for systems that do not support two-factor authentication should be rotated every 90 days.
- Passwords should be unique passwords per system and passwords should be different from the last 4 passwords used in the system.
- Access to Rethink customer administrative functions further require two-factor authentication.
- Multi-Factor Authentication will be enabled and utilized to further enhance the security of a system.

## Authorized Use Policy

With the exception of information published for public consumption, all users of Rethink's information systems must be formally authorized by appointment as a member of staff, or by another process specifically authorized by the CEO, Privacy Officer, or Management Level staff. Authorized users will be in possession of a unique user identifier ("User ID"). An authorized user must not share the password associated with his or her User ID with any other person. Each authorized user is responsible for all activities conducted using his or her User ID. Rethink utilizes the "Principle of least privilege" to ensure access is only granted with the minimum rights/ information needed to complete job duties. A user's role will determine the access granted in Rethink's information systems. All users are responsible for the security of data, accounts, and systems under their control.

## Information Systems Owners

Administrators who are responsible for information systems are required to ensure that:

1. Systems are adequately protected from unauthorized access.
2. Systems are secured against theft and damage to a level that is cost-effective.



3. Adequate steps are taken to ensure the availability of the information system, commensurate with its importance (Business Continuity).
4. Electronic data can be recovered in the event of loss of the primary source, i.e., failure or loss of a computer system. It is incumbent on all system owners to backup data and to be able to restore data to a level commensurate with its importance (Disaster Recovery).
5. Data is maintained with a high degree of accuracy.
6. Systems are used for their intended purpose and that procedures are in place to rectify discovered or notified misuse.
7. Any electronic access logs are only retained for a justifiable period to ensure compliance with the data protection, investigatory powers, and freedom of information acts.
8. Any third parties entrusted with Rethink's data understand their responsibilities with respect to maintaining its security.
9. Quarterly access reviews are conducted and users who no longer need access to the system are removed from the system.

## Risks/Liabilities/Disclaimers

Rethink reserves the right to disconnect company devices or disable services without notification.

Rethink has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted while on company business.

Lost or stolen company devices must be reported to Rethink within 12 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.

The employee is expected to always use his or her devices in an ethical manner and adhere to Rethink's acceptable use policy as outlined above.

Rethink reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

## Software Security

Object and source code for system software shall be securely stored when not in use by the developer. Developers will not have access to modify program files that actually run in production. Changes made by developers must be implemented into production via the change management process. Unless access is routed through an application interface, no developer shall have more than read access to production data.

Open-Source Software may be used at times by developers and blend proprietary and open software development. When deciding upon open-source solutions, maintainability and vulnerability management will be factored in before use. The Head of Software will have oversight on how and if the software will be permitted to be utilized in the production environment. Open-Source Licenses will be reviewed prior to usage as well for the consideration of the software.

Public and private keys shall be protected against unauthorized modification and substitution.

Procedures shall be in place to ensure proper generation, handling, and disposal of keys as well as the destruction of outdated keying material.

Procedures shall be in place to safeguard all cryptographic material, including certificates.

## Cloud Computing and External Services Policy

---

Cloud computing offers a number of advantages including low costs, high performance, quick delivery of services and location independence. However, without adequate controls, it also exposes Rethink, its employees and its partner organizations to online threats such as data loss or theft, unauthorized access to corporate networks, and so on.

This Cloud Computing and External Services Policy is meant to ensure that cloud services are NOT used without Rethink's knowledge and approval. It is imperative that employees NOT open cloud services or any online accounts or enter into contracts for the storage, manipulation or exchange of company-related communications or company-owned data without the approval of the Controller or CEO. This is necessary to protect the integrity, security, and confidentiality of Rethink's data.

Rethink remains committed to enabling employees to do their jobs as efficiently as possible through the use of technology. The following guidelines are intended to establish a process whereby Rethink employees can use cloud services without jeopardizing company data and computing resources.

### Scope

This policy pertains to all external services, e.g., cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. Personal accounts should never be used to secure company services, and therefore are excluded.

If you are not sure whether a service is covered under this section, please contact the Rethink Privacy Officer.

### Policy

Use of cloud computing services for work purposes must be formally authorized by the Rethink Privacy Officer or CEO. The Rethink Privacy Officer will certify that security, privacy, and all other IT management requirements will be adequately addressed by the vendor.

For any services that require users to agree to terms of service, such agreements must be reviewed and approved by the Rethink Privacy Officer, CEO, and/or CFO.

The use of such services must comply with all Information Services Policies.

Employees must not share login credentials with co-workers. The Controller will keep a confidential document containing account information for business continuity purposes.

The use of such services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by Rethink.

Personal cloud services accounts may not be used for the storage, manipulation or exchange of company-related communications or company-owned data.



## Data Retention Policy

---

### Company Data

Although Rethink is primarily paperless, these policies apply uniformly to documents retained in either paper or electronic format (including email communications).

We retain business records to comply with Internal Revenue Service (IRS) and associated federal and local regulations and to retain all documentation necessary to support our work, our correspondence with customers, our work product, customer bills, invoices & payment information, and anything else of continuing significance or required by contract, statute, rule, or regulation. Drafts or other documents not utilized should not be retained. Documents transmitted as attachments via email should be considered separately from the email messages to which they are attached.

How do we store & protect customer data?

Documents attached to and transmitted by email are stored in machine readable format in our electronic document management systems, currently OneDrive, Dropbox, and DriveHQ. Email messages are retained in Office365 and are not routinely retained.

### Retention Duration

#### Rethink Business Records

We retain the following business records for a period of seven (7) years: annual general ledger detail, annual financial reports, bank statements & cancelled checks, depreciation schedules, payroll data, vendor invoices & paid bills, W-2 & 1099 forms, accident reports & claims, firm publications, advertising & promotional materials (including customer newsletters & alerts), work sheets & related backup documents for tax returns, accounts receivable reports, customer billing statements, insurance documents & policies, leases & contracts, and personnel files. Calculation of the retention period for records covering a stated duration, or finite period of time begins to run at the end of the term, expiration, or period of employment.

#### Customer Administrative Records

We retain the following customer records for a period of seven (7) years, or at the end of the contract: annual financial statements, audit reports, bookkeeping & payroll files, financial statements, tax returns, tax audit or other IRS-related documents, reports from government agencies, other regulatory & accreditation bodies or organizations, valuations.

### Disposal

It is our policy to destroy files after the expiration of their respective retention period. The customer or former customer is responsible for any costs associated with document retrieval, printing, or duplication. In the case of tax returns and workpapers, retention periods commence immediately following the date of the financial statements or the taxable year.



Paper documents not to be retained are securely shredded. Any paper with a social security number, a federal ID number (FEIN) or a customer name on it is destroyed in this manner. Electronic documents are destroyed by deleting them from the medium on which they are stored, and then purging the medium itself. Financial and Other Business Documents will be destroyed utilizing machines that are a Security Level P-3 or greater. Any documents that contain Personal Identifiable Information will be destroyed utilizing a Security Level P-4 machine or greater.

### Customer Data

Customer data, including user data, engagement activity and analytics information, are retained within Rethink for up-to 7 years at which point personal information will be purged from the record. Customer-specific variances from Rethink's data retention requirements are documented by individual customer agreements with Rethink.

At times, staff may need to work with Customer data that contains personal data. During processing of personal data, users may not utilize any tools that are not a part of Rethink's list of approved software and vendors. Personal data should be used for the duration necessary and deleted from the system once complete. Staff who need to utilize a specific tool for processing, must request a risk assessment and review of the new vendor or tool prior to using the tool.

## Information Classification Policy

---

All Rethink employees are expected to review this information classification policy and to consistently apply information classifications in their daily business activities.

Rethink's information classification approach is based on the concept of 'need to know.' This means that information is not disclosed to any person who does not have a legitimate business need to receive the information. This concept is intended to protect information entrusted to Rethink from unauthorized disclosure, use, modification, and deletion.

This information classification policy is applicable to all electronic information managed by Rethink, both internal and customer related.

### Access Control

An employee who is unclear how this policy should be applied to any particular circumstance should conservatively apply the 'need to know' concept - the information must be disclosed only to those people who have a legitimate business need for the information.

### System Access Controls

The proper controls shall be in place to authenticate the identity of users and to validate each user's authorization before allowing the user to access information or services on the system including administrative functions. Rethink administrators will ensure that only personnel with the proper authorization and a need to know are granted access to Rethink systems and resources. Access in all cases shall be controlled through identification and authentication mechanisms.

Information at Protection Levels 2 or 3 is provided to an individual only after the authorization of the Rethink Privacy Officer or CEO has been obtained.

## Information Classification

Classification	Data Class	Adverse Business Impact	Sample Data (not an exhaustive list)
Highly Confidential Information	Protection Level 3	Extreme	Data that creates extensive "shared-fate" risk between multiple sensitive systems, e.g., enterprise credential stores and central system management consoles.
Confidential Information	Protection Level 2	High	<p>Data elements with a statutory requirement for notification to affected parties in case of a confidentiality breach:</p> <ul style="list-style-type: none"> <li>• Customer-classified personal information</li> <li>• Individual passwords</li> <li>• Personal medical or health information</li> <li>• Identifiable content engagement information</li> <li>• Content Subscriptions</li> </ul>
Internal Use Only	Protection Level 1	Moderate	<p>Information intended for release only on a need-to-know basis, including Rethink company information and customer personal information not otherwise classified as Level 0, 2 or 3, and information protected or restricted by contract, grant, or other agreement terms and conditions, e.g.:</p> <ul style="list-style-type: none"> <li>• Rethink content</li> <li>• System event information</li> <li>• Non-identifiable engagement information</li> <li>• Individual member and/or employee ID</li> <li>• Sponsor-related information such as working location</li> <li>• Sales-related information</li> </ul>



Non-Confidential Information	Protection Level 0	Limited or none	Information intended for public access, e.g.: <ul style="list-style-type: none"><li>• Information about Rethink and its offerings</li><li>• Course summaries, teacher biographies, etc.</li><li>• Selected non-identifiable and aggregated analytics</li><li>• Public policies</li></ul>
------------------------------	--------------------	-----------------	--

All electronic information managed by Rethink has a designated Owner, who is responsible for assigning appropriate sensitivity classifications. Owners do not legally own the information entrusted to their care. They are instead designated individuals who act as stewards, and who supervise the ways in which certain types of information are used and protected. Data Owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put.

Information at Protection Levels 2 or 3 should be stored only on enterprise-level servers. Such information may not be stored on a personal computer, portable computer, smartphone, tablet, removable media, or other single-user system without the permission of the Rethink Privacy Officer or CEO. Rethink employees must not install encryption software to encrypt files or folders without the express written consent of the CEO.

## Information Transfer

Restricted information transmitted over any external communication network may be sent only in encrypted form. Such networks include SFTP or other secure transfer methods. All such transmissions must use a virtual public network or similar software as approved by the Rethink Privacy Officer.

## Media Protection and Data Handling Policy

### Purpose

The quality and integrity of Rethink's media protection mechanisms allow information a greater level of security than can be achieved with system-based protection mechanisms alone. Without media protection mechanisms, Rethink's data, information, and other media assets could be exposed to an unnecessarily high level of risk, particularly in circumstances where that information is taken out of the information system.

## Scope

The Media Protection Policy applies to all Rethink employees, including all temporary or contract workers. Specifically, it applies to all email accounts provided by Rethink and all email transmissions made over Rethink networks and network services. Further, this includes:

- Removable magnetic media including external hard disk drives, external devices containing hard disk drives, floppy disks, and magnetic tape.
- Removable flash-based media including thumb drives, digital media players, digital cameras, and smart phones or cell phones.
- Optical media including DVDs and CDs.
- Collateral, paper, and other printable materials.

## Definitions

**Non-Privileged Information** - Information or data that is classified as Non-Confidential (Protection Level-0).

**Privileged Information** - Information or data that is classified as Highly Confidential (Protection Level-3), Confidential (Protection Level-2), or Internal Use Only (Protection Level-1).

**Removable Media** - Includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, and digital video disks) and non-digital media (e.g., paper, microfilm).

## Governing Laws and Regulations

Guidance	Section
SOC 2	
NIST SP 800-800	4.1 -4.8
NIST SP 800-53 v4	PE-2–PE-6, MA-5, PE-8, CP-2, CP-6, CP-7, PE-1, CP-8, PE-19–PE-16, MA-2–MA-6, AC-19, AC-20, MP-5, PE-17, MP-6, MA-2, MP-5
NIST SP 800-171	3.8.1-3.8.9



## Policy Statements

### Basic Security Requirements:

- All privileged information when stored out of system (via information media) will be protected by media protection mechanisms to ensure the highest levels of security. Non-privileged information (NPI) will be protected to ensure the highest levels of integrity and availability.
- Protect (i.e., physically control and securely store) information system media containing information, both paper and digital.
- Rethink will limit access to information on information system media to authorized users.
- Information system media containing information will be sanitized or destroyed before disposal or release for reuse.
- The destruction of the Information system media will adhere to guidance of NIST.

### Derived Security Requirements:

- Rethink will mark media with necessary information classification markings and distribution limitations.
- Where information is transferred to the media, that media shall be stored securely within a controlled area and access to that controlled area shall be physically restricted to authorized personnel. Further, the mechanisms that enforce those access restrictions shall collect access information and shall include the ability to audit access attempts.
- Cryptographic mechanisms shall be implemented to protect the confidentiality of information stored on digital media during transport unless otherwise protected by alternative physical safeguards.
- Rethink will control the use of removable media on information system components.
- When content from the information system is output to some form of media, that content and media must be handled and stored in a secure manner.
- Rethink will control access to media containing information and maintain accountability for media during transport outside of controlled areas. Further, all such transportation shall be documented.
- The use of portable storage devices will be prohibited when such devices have no identifiable owner.

## Security Awareness Training Policy

---

### Purpose

The quality and integrity of Rethink's security awareness training ensures that the workforce members, including management of Rethink's information systems, understand the security implications of their actions and increases the likelihood that information system security will not be breached, either intentionally or unintentionally, through technical measures (such as hacking) or non-technical measures (such as social engineering).

The goal is to ensure users understand the risks of using information technology, how to defend against malicious threats, and how to react to information security events or incidents, whether at work or at home. Without such training, information systems users have an increased likelihood of breaching security and have lower individual culpability should they breach security.

### Scope

This Security Awareness Training Policy applies to all users of all information systems that are the property of Rethink. Specifically, it includes:

- All employees, whether employed on a full-time or part-time basis by Rethink.
- All contractors and third parties that work on behalf of and are paid directly by Rethink.
- All contractors and third parties that work on behalf of Rethink but are paid directly by an alternate employer.
- All employees of partners and clients of Rethink that access Rethink's non-public information systems.

### Definitions

**IT Security Awareness Training:** A formal process for educating employees about computer security.

**Breach:** Any incident that results in unauthorized access of data, applications, services, networks, and/or devices by bypassing their underlying security mechanisms.



### Governing Laws and Regulations

Guidance	Section
SOC 2	CC1.4
SOC 2	CC2.2
SOC 2	CC2.3
GDPR	Article 35

### Policy Statements

#### Basic Security Requirements:

- Rethink will ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.
- Ensure that organizational personnel are adequately trained to carry out their assigned information-security-related duties and responsibilities.

#### Derived Security Requirements:

- Security awareness training will be provided to ensure all parties within the scope of this policy can recognize and report potential indicators of insider threat.
- Upon completion of security awareness training, all employees will be required to sign a declaration that they have completed training, understand the purpose of the training and the specific procedures taught, and that they intend to abide by Rethink's security policies.
- All employees of Rethink that work as administrators or hold other positions with significant and relevant security operations responsibilities are required to participate in security operations training within 30 days of starting work or the deployment of a new or significantly updated/revised information system and thereafter on an annual basis. Upon completion of security operations training, all employees will be required to sign a declaration that they have completed the training, understand the purpose of the training and the specific procedures taught, and that they intend to abide by Rethink's security policies.

Security training will be ongoing at Rethink. Employees will be kept up to date on new improvements or threats to watch out for. These can be distributed by, but not limited to, email, collaboration tools, posters, work newspapers, or meetings.



## System Configuration Management Policy

---

### Purpose

The quality and integrity of Rethink’s standardized configuration settings allow information systems and information system components to be consistently deployed in an efficient and secure manner. Without standardized configuration settings, the potential exists that information systems may be deployed that fail to meet the security requirements of Rethink, or that compromise the security requirements of other information systems with which they interconnect.

### Scope

This Systems Configuration Management Policy applies to all information systems and information system components of Rethink. Specifically, it includes:

- Servers, and other devices that provide centralized computing capabilities.
- SAN, NAS, and other devices that provide centralized storage capabilities.
- Desktops, laptops, and other devices that provide distributed computing capabilities.
- Routers, switches, and other devices that provide network capabilities.
- Firewalls, IDP sensors, and other devices that provide dedicated security capabilities.

### Definitions

**Configuration Baseline:** Configuration information formally designated at a specific time during a product’s or product component’s life.

**Security Impact Assessment:** Analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.

### Governing Laws and Regulations

Guidance	Section
NIST SP 800-171	3.4.1-3.4.9
SOC 2	CC8.1

## Policy Statements

### Basic Security Requirements:

- Configuration baselines and inventories will be established and maintained of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development lifecycles.
- Rethink will establish and enforce security configuration settings for information technology products employed in organizational information systems.
- Rethink will conduct a review and implementation of hardening guidelines of the information system prior to deployment.

### Derived Security Requirements:

- Rethink will track, review, approve/disapprove, and audit changes to information systems.
- Rethink will analyze the security impact of changes prior to implementation.
- Rethink will define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.
- The principle of least functionality will be employed by configuring the information system to provide only essential capabilities.
- Networks will be configured to restrict information flow between information systems or components of information systems through the use of access control lists.
- Rethink will restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.
- Rethink will apply deny-by-exception (blacklist) processes to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) processes to allow the execution of authorized software.
- Rethink will analyze changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.
- An asset inventory of information system components will be maintained. The inventory will be updated when a new information system or information system component is implemented or an old one is retired.
- Emergency changes to an information system must be minimally documented and authorized and performed in a controlled manner.
- User-installed software will be controlled and monitored.

## System Maintenance Policy

---

### Purpose

The quality and integrity of Rethink’s information system maintenance is required to ensure that information systems are always operating optimally. Set maintenance processes are required to ensure that maintenance is conducted in the most secure manner possible. Without systems maintenance, the potential exists that information systems will be unable to provide appropriate information security. Without maintenance processes, the potential exists that the act of performing systems maintenance could, either directly or indirectly, compromise information system security.

### Scope

The System Maintenance Policy applies to all information systems and information system components of Rethink. Specifically, it includes:

- Mainframes, servers, and other devices that provide centralized computing capabilities.
- SAN, NAS, and other devices that provide centralized storage capabilities.
- Desktops, laptops, and other devices that provide distributed computing capabilities.
- Routers, switches, and other devices that provide network capabilities.
- Firewalls, IDP sensors, and other devices that provide dedicated security capabilities.

### Definitions

**Multi-Factor Authentication (MFA):** A security system that requires more than one method of authentication from independent categories of credentials to verify the user’s identity for a login or other transaction.

**Secure Shell (SSH):** A cryptographic network protocol for operating network services securely over an unsecured network.

### Governing Laws and Regulations

Guidance	Section
SOC 2	



## Policy Statements

### Basic Security Maintenance and Integrity Requirements:

- Rethink will perform maintenance on organizational information systems.
- Rethink will provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
- Rethink will identify, report, and correct information and information system flaws and vulnerabilities in a timely manner not to exceed 1 month.
- Rethink will provide protection from malicious code at appropriate locations within organizational information systems.
- Security vulnerabilities will be ranked based on risk level including identification of "high risk" and "critical" vulnerabilities.
- Rethink will monitor reputable outside sources for information system security alerts and advisories and appropriate actions will be taken in response.

### Derived Security Requirements:

- All media containing diagnostic and test programs will be checked for malicious code before the media are used in the information system.
- Only pre-authorized personnel are allowed to perform information system maintenance.
- Multi-factor authentication or secure network session via SSH or access token is required to establish nonlocal maintenance sessions via external network connections; terminate such connections when nonlocal maintenance is complete.
- Remote maintenance must be authorized, actively monitored, and audited upon completion.
- Rethink will supervise the maintenance activities of maintenance personnel without required access authorization.
- A maintenance log shall be maintained for all information system maintenance.
- Malicious code protection mechanisms are updated when new releases are available.
- System Patches will be prioritized based on severity and risk of the component to be patched.
- Rethink will perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed to identify new security vulnerabilities.
- Rethink will monitor the information system, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
- Unauthorized uses of the information system are identified.

## Vulnerability Management and Security Assessment Policy

---

### Purpose

The quality and integrity of Rethink's security assessment is focused on determining the degree to which information system security controls are correctly implemented, whether they are operating as intended, and whether they are producing the desired level of security. Vulnerability assessment is focused on determining the weaknesses inherent in the information systems that could be exploited, leading to an information system breach. Without security and vulnerability assessments, the potential exists that information systems may not be as secure as intended or desired.

### Scope

This Vulnerability Management and Security Assessment Policy applies to all information systems and information system components of Rethink. Specifically, it includes:

- Servers, and other devices that provide centralized computing capabilities.
- SAN, NAS, and other devices that provide centralized storage capabilities.
- Desktops, laptops, and other devices that provide distributed computing capabilities.
- Routers, switches, and other devices that provide network capabilities.
- Firewalls, IDP sensors, and other devices that provide dedicated security capabilities.

### Definitions

**Continuous Monitoring:** A program that allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions or business processes.

### Governing Laws and Regulations

Guidance	Section
SOC 2	CC7.1
SOC 2	A3.8
SOC 2	S3.5

## Policy Statements

### Basic Security Requirements:

- Rethink will periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.
- While both security and vulnerability assessments are to be performed by internal staff on an ongoing basis, third parties will be retained yearly to ensure appropriate levels of coverage and oversight.
- Rethink will develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.
- Vulnerabilities and security issues identified with a "critical-risk" or "high-risk" severity level will be prioritized and remediated in a feasible timely manner.
- Information system security controls will have continuous monitoring on an ongoing basis to ensure the continued effectiveness of the controls.
- Rethink will monitor service critical vendors for security patches to correct deficiencies and reduce or eliminate vulnerabilities in third-party integrations and services.

## Change Management Policy

---

### Overview

Operational change management brings discipline and quality control to Engineering. Attention to governance and formal policies and procedures will ensure its success. Adopting formalized governance and policies for operational change management delivers a more disciplined and efficient infrastructure. This formalization requires communication; the documentation of important process workflows and personnel roles; and the alignment of automation tools, where appropriate. Where change management is nonexistent, it is incumbent on Information Security's senior management to provide the leadership and vision to jump-start the process. By defining processes and policies, Engineering can demonstrate increased agility in responding predictably and reliably to new business demands.

Rethink management has recognized the importance of change management and control and the associated risks with ineffective change management and control and have therefore formulated this Change Management Policy in order to address the opportunities and associated risks.

### Purpose

The purpose of this policy is to establish management direction and high-level objectives for change management and control. This policy will ensure the implementation of change management and control strategies to mitigate associated risks such as:

- Information being corrupted and/or destroyed;
- Computer performance being disrupted and/or degraded;
- Productivity losses being incurred; and
- Risk exposure to Rethink's reputation



The Change Management Policy ensures that changes fulfill business operations requirements and comply with legal and regulatory requirements. In addition, the Change Management Policy manages changes in a rational and predictable manner so that the business can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce the potential for negative impact to the users, partners, and the business.

## Scope

This policy applies to all parties operating within Rethink's network environment or utilizing Information Resources. It covers the data networks, servers, and personal computers (stand-alone or network-enabled) located at Rethink offices and Rethink production related locations, where these systems are under the jurisdiction and/or ownership of the company, and any personal computers, laptops, mobile device and or servers authorized to access the company's data networks. No employee is exempt from this policy.

## Definitions and Abbreviations

**Audit trail:** A record or series of records which allows the processing carried out by a computer system to be accurately identified, as well as verifying the authenticity of such amendments.

**BCP:** Business Continuity Plan

**DR:** Disaster Recovery

**Information resources:** All data, information as well as the hardware, software, personnel, and processes involved with the storage, processing, and output of such information. This includes data networks, servers, PC's, storage media, printer, photocopiers, fax machines, supporting equipment, fallback equipment, and back-up media.

**Method of Procedure (MOP):** A step-by-step sequence for performing an operation.

**SLA:** Service Level Agreement

## Governing Laws and Regulations

Guidance	Section
NIST SP 800-53	CM-1, CM-3, CM-4

## Policy Statements

Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorized, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.

In order to fulfill this policy, the following statements shall be adhered to:

### *Operational Procedures*

The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all critical company information resources (such as hardware, software, system documentation and operating procedures). This documented process shall include management responsibilities and procedures. Wherever practicable, operational and application change control procedures should be integrated.

At a minimum the change control process should include the following phases:

- Logged Change Requests
- Identification, prioritization and initiation of change
- Proper authorization of change
- Requirements analysis
- Inter-dependency and compliance analysis
- Impact Assessment
- Change Method-of-Procedure (MOP)
- Change testing
- User acceptance testing and approval
- Implementation and release planning
- Documentation
- Change monitoring
- Defined responsibilities and authorities of all users and personnel

### *Documented Change*

All change requests shall be logged whether approved or rejected on a standardized and central system. The approval of all change requests and the results thereof shall be documented.

A documented audit trail, containing relevant information shall be maintained at all times. This should include change request documentation, change authorization and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorized personnel.

### *Risk Management*

A risk assessment shall be performed for changes and dependent on the outcome, an impact assessment should be performed.

The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.

### *Change Classification*

All change requests shall be prioritized in terms of benefits, urgency, effort required and potential impact on operations.



### *Testing*

Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimize the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.

### *Changes affecting SLA's*

The impact of change on existing SLA's shall be considered for alignment with existing service provider SLA's.. Where applicable, changes to the SLA shall be controlled through a formal change process which includes contractual amendments.

### *Version control*

Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies.

### *Approval*

All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e., the change request was done by an authorized user, the impact assessment was performed, and proposed changes were tested.

### *Communicating changes*

All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change. Users shall be required to make submissions and comment prior to the acceptance of the change.

### *Implementation*

Implementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes. (For more information see System Development Life Cycle)

### *Fall back*

Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert to what they were prior to implementation of changes.

### *Documentation*

Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.



Information resources documentation is used for reference purposes in various scenarios, i.e. further development of existing information resources as well as ensuring adequate knowledge transfer in the event of the original developer and/or development house being unavailable. It is therefore imperative that information resources documentation is complete, accurate and kept up to date with the latest changes. Policies and procedures, affected by software changes, shall be updated on completion of each change.

### *Business Continuity Plans (BCP)*

Business continuity plans shall be updated with relevant changes, managed through the change control process. Business continuity plans rely on the completeness, accuracy and availability of BCP documentation. BCP documentation is the road map used to minimize disruption to critical business processes where possible, and to facilitate their rapid recovery in the event of disasters.

### *Emergency Changes*

Specific procedures to ensure the proper control, authorization, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.

### *Change Monitoring*

All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

### *Change Requests*

All requests should occur for any changes that affect customers, end-user experience, sensitive data/information, system operations, or are a high risk to the organization. Requests will be documented in the #team-cab Rethink Slack Channel for documentation purposes and tracking of changes.

#### **Change Description:**

**Date:** [Change will occur]

**MOP:** [Include the steps and who is assigned to each step]

#### **Monitoring Plan:**

**Rollback:** [Reverse Changes if Necessary]

**CS Impact:** [Description of Impact]

**System Impact:** [Description of Impact]

**CS Risk:** [LOW/MEDIUM/HIGH]

**Security Risk:** [LOW/MEDIUM/HIGH]

#### **Approval by Rethink's CAB Team.**

Dialogue should be in Slack thread format to keep the conversation organization within the change request.

## Software Development Life Cycle

---

### Purpose

The purpose of the Software Development Life Cycle (SDLC) policy is to document the requirements for developing and/or implementing new software and systems at Rethink and to ensure that all development work is compliant as it relates to: (i) any and all regulatory, statutory, international, federal, and /or state guidelines, and (ii) any and all Rethink contractual obligations.

### Scope

This policy applies to all employees at Rethink and other covered individuals (contractors, 3rd party services, etc.) that perform any type of software or systems development work at Rethink.

### Definitions

**Design Document:** A written description of a software product, that a software designer writes to give a software development team an overall guidance of the architecture of the software project.

**Quality Assurance (QA) testing** provides an objective, independent view of the software through various testing tools and methodologies, to allow Rethink to appreciate and understand the risks at implementation of the software.

**Security Assessment testing** utilizes automated and/or manual means to assess the security of an application or system. While similar to QA testing, the focus of this testing is to find potential security vulnerabilities and threats before full implementation.

#### Governing Laws and Regulations:

Guidance	Section
NIST SP 800-53	CM-1,CM-3, CM-4

### Policy Statements

The Product and Engineering team at Rethink is responsible for developing, maintaining, and participating in a Software Development Life Cycle for software and systems development projects. All entities at Rethink engaged in systems or software development activities must follow the SDLC.

Software and Systems developed at Rethink utilize the Agile Software Development model to meet the following principles of agile development: Plan, Sprint, Ship. Repeat. Maintain.



- Plan: Define and document feature requirements with business and customer input. Prioritize features in a backlog.
- Sprint: Determine features that can be completed during a defined sprint period of two weeks. Develop these features in a testable manner using QA and DEV environments.
- Ship: Shippable software is released to users.
- Operations: Maintenance and monitoring of applications and systems

To meet the principles outlined, Rethink implements a number of phases that are repeated in cycles, with feedback loop after each cycle is completed. The product and engineering team learns from preceding cycles and plans the next cycle in an attempt to converge on an acceptable solution. At the discretion of the business, the product team may release a partial solution for specific features. The characteristics of Agile development that Rethink abides by include:

- Iterative structure - structured around iterations that are designed to find and complete the solution in a fixed timeframe
- Just-in-time planning - highest importance features are prioritized at each sprint. Planning is finely detailed for immediate features, coarsely detailed for features to be developed later.
- Thrives on change through learning and discovery
- Staffing project teams with a focus on resource versatility so that the core group can fill multiple roles and have a wider view of the overall approach.

Additionally, Software and Systems development at Rethink will adhere to the following:

- All development work shall exhibit a separation between development, QA, and production environments unless prohibited by licensing restrictions or an exception is made. Separate environments allow better management and security for the production systems, while allowing greater flexibility in the pre-production environments.
- At a minimum, a software development plan should address the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; general design; detail design; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used in conjunction with critical and/or sensitive Rethink information.
- Where these separation distinctions in environments have been established, development, and development/QA/test staff must not be permitted access to production systems unless absolutely required by their respective job duties/descriptions.
- All software code developed in-house must be planned, reviewed, version controlled, quality assured, released and monitored through the established mechanisms developed at Rethink.
- Documentation will be kept and updated during all phases of development from the initiation phase through implementation and ongoing maintenance phases. Additionally, security considerations should be noted and addressed through all phases.

# Wireless Setup and Access Policy

---

## Overview

Wireless technology provides a mechanism for accessing Internet resources easily without tied to a wired connection at user's desk. These technologies have become ubiquitous in the workplace environment. Wireless technologies at work adds increased functionality but also adds security risks and concerns that must be managed and mitigated.

## Purpose

This policy provides a set of procedures and standards for implementing wireless technologies within Rethink network environment. It provides network administrators who deploy and manage wireless technologies with a baseline set of requirements that document connectivity, security, and device oversight.

## Scope

This policy applies to all Rethink employees who use, install or support wireless networks.

## Policy

### Introduction

By using wireless devices within Rethink network for business purposes, all employees are subject to policies managing their use. All wireless devices including personal smartphones, tablets, or other devices are subject to the guidelines and procedures set forth in this policy.

### Connectivity Considerations

The following procedures and practices shall be implemented to reduce risks related to wireless networks:

- Wireless networks shall be segmented between external guest and internal networks. Non-Rethink devices shall not be connected to the Rethink's internal network.
- Users inside the Rethink firewall shall not connect to the internal network if they are using a bridged wireless connection to connect to an external network.
- Wireless access points or routing devices with wireless capability are not allowed unless approved by the SecOps / IT Analyst
- Logical and physical user access to wireless network devices shall be restricted to authorized personnel and devices excepting for access to a guest network
- Perimeter firewalls shall be implemented and configured by support staff to restrict unauthorized access and traffic metering
- All vendor default settings for wireless devices (e.g., passwords, wireless encryption keys, SNMP community strings) shall be changed prior to installing wireless equipment in Rethink environment
- Wireless security protocols shall be used that are of the highest encryption possible



- Strong passwords shall be employed for all wireless SSID and changed on a periodic basis either through the protocol or across Rethink
- Ad-hoc Rethink wireless device audits shall be conducted on at least a quarterly basis to determine if any rogue devices exist on the Rethink network
- Findings shall be presented immediately to the senior management and all rogue devices removed from the network

## Security

Wireless (Wi-Fi) transmissions used to access Rethink networks and devices shall be encrypted. If sent across a public or open network, both the authentication data (e.g., a user ID and password) and the data itself shall be encrypted with strong encryption. Data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission security protocols along with approved encryption techniques are utilized.

The Security Analyst shall ensure:

- Sensitive information is encrypted using the strongest and most cost-effective encryption available
- Wireless networks transmitting sensitive information or connected to sensitive information environments, use industry best practices to implement strong encryption for authentication and transmission
- Processes test for the presence of rogue wireless access points and detect and identify all authorized and unauthorized wireless access points
- Procedures maintain an inventory of authorized wireless access points including a documented business justification
- Response procedures exist and are implemented in the event unauthorized wireless access points are detected
- Older encryption protocols such as Wired Equivalent Privacy (WEP) or SSL are not used for authentication or transmission

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of Rethink. Satisfactory examples of evidence and compliance include:

- Spot user checks for compliance with this policy
- Archival documentation of quarterly checks and any remediation required
- Anecdotal communication evidence of policy implementation via email, logs, or other documentation

## BYOD Policy

---

### Objective

This policy establishes Rethink guidelines for employee use of personally owned electronic devices for work-related purposes.

## Scope

Employees of Rethink are allowed to use only Rethink supplied laptops and computers on Rethink HQ network. In some exceptional cases, employees may have the opportunity to use their personal electronic devices for work purposes when authorized in writing, in advance, by the employee and management. Personal electronic devices include personally owned cellphones, smartphones, tablets, laptops, and computers.

The use of personal devices is limited to certain employees and may be limited based on compatibility of technology. Contact the human resource (HR) department for more details.

## Procedure

### Device protocols

To ensure the security of Rethink information, authorized employees are required to have Sophos anti-virus installed on their personal laptops.

Employees may store company-related information only in Rethink supplied laptops. Employees may not use cloud-based apps or backup that allows company-related data to be transferred to unsecure parties. Due to security issues, personal devices may not be synchronized with other devices in employees' homes. Making any modifications to the device hardware or software beyond authorized and routine installation updates is prohibited unless approved by IT. Employees may not use unsecure Internet sites.

### Restrictions on authorized use

Employees whose personal devices have camera, video or recording capability are restricted from using those functions anywhere in the building or on company property at any time unless authorized in advance by management.

While at work, employees are expected to exercise the same discretion in using their personal devices as is expected for the use of company devices. Rethink policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information and ethics apply to employee use of personal devices for work-related activities.

Nonexempt employees may not use their personal devices for work purposes outside of their normal work schedule without authorization in advance from management. This includes reviewing, sending and responding to e-mails or text messages, responding to phone calls, or making phone calls.

An employee may not store information from or related to former employment on the company's application.

Family and friends should not use personal devices that are used for company purposes.

### Privacy/company access

No employee using his or her personal device should expect any privacy except that which is governed by law. Rethink has the right, at any time, to monitor and preserve any communications that use Rethink's networks in any way, including data, voice mail, telephone logs, Internet use and network traffic, to determine proper use.

Management reserves the right to review or retain personal and company-related data on personal devices or to release the data to government agencies or third parties during an investigation or litigation. Management may review the activity and analyze use patterns and may choose to publicize these data to ensure that Rethink's resources in these areas are being used according to this policy. Furthermore, no employee may knowingly disable any network software or system identified as a monitoring tool.

## Safety

Employees are expected to follow applicable local, state, and federal laws and regulations regarding the use of electronic devices at all times.

Employees whose job responsibilities include regular or occasional driving are expected to refrain from using their personal devices while driving. Regardless of the circumstances, including slow or stopped traffic, employees are required to pull off to the side of the road and safely stop the vehicle before placing or accepting a call or texting. Special care should be taken in situations involving traffic, inclement weather, or unfamiliar areas.

Employees who are charged with traffic violations resulting from the use of their personal devices while driving will be solely responsible for all liabilities that result from such actions.

Employees who work in hazardous areas must refrain from using personal devices while at work in those areas, as such use can potentially be a major safety hazard.

## Lost, stolen, hacked or damaged equipment

Employees are expected to protect personal devices used for work-related purposes from loss, damage or theft.

Rethink will not be responsible for loss or damage of personal applications or data resulting from the use of company applications or the wiping of company information. Employees must immediately notify management in the event their personal device is lost, stolen or damaged. If it is unable to repair the device, the employee will be responsible for the cost of replacement.

Employees may receive disciplinary action up to and including termination of employment for damage to company issued devices caused willfully by the employee.



## Lost media or laptop

---

When laptop is lost or recovered from being stolen:

- Was the laptop encrypted?
- What data was on the laptop?
- Was it turned off or locked when it was stolen or lost?
- What remote access did the employee have?
- If they did have remote access, should you disable or suspend these accounts until passwords can be reset? Do you know how to get that done in a hurry?
- Who needs to be informed of the incident? Should you tell management? Report it to the police?

Immediately initiate incident response by creating an incident report. Write the details of next steps to resolve the issue.

## Early Access Policy

---

### Objective

This policy establishes Rethink guidelines for early access to Rethink resources to a future employee. Usually, this access is granted no more than 1 week prior to joining Rethink. This helps with smooth on-boarding and makes them productive from day 1 at Rethink.

### Scope

Future employee of Rethink is allowed to use only Rethink email for easier communication with HR and senior management prior to on-boarding. Office365 is monitored for security.

### Procedure

1. Future employees agree to not share any information shared in Rethink's email account.
2. Future employee signs NDA agreement. They can't forward or download information shared through Rethink's email.
3. Rethink employees who are coordinating and communicating with future employees should make sure that they are not sharing any sensitive or personal information with future employees. Only process related information can be shared.
4. In the case of a future employee who decides to not join Rethink in the last moment or if Rethink decides to not continue with the future employee's on-boarding, Office365 access is revoked immediately.

## Release Management Policy

---

### Overview

The Release Management Policy defines the process and steps that must be followed when making a change in the Rethink Production environment. This includes updates to code, changes in AWS resources such as security groups, Bastion host(s), data pipelines, or anything that impacts the functionality or performance of the production environment. This policy should be reviewed and updated during the first week of each quarter.

### Purpose

This policy requires that changes to software or other resources in the production environment are coordinated and logged to prevent service disruption, duplication of effort, or conflict. Additionally, it will help ensure that changes are tracked which will be useful for debugging problems discovered after changes are made.

## Standard Change Process

The following rules must be followed when making changes to the Rethink platform in production:

- A Jira ticket must be created for all changes made to the Rethink platform
- All releases must be pre-approved by Product Management
- Rollback plans must be in place before the production system is modified
- Changes must be verified in the staging environment before released into production
- Changes requiring new documentation must be released with said documentation
- Code changes must be committed to a master branch in GitHub before being released • Code released into production must be built by a centralized build machine

## Hotfix Change Process

High-priority hotfixes should follow the same Standard Change Process steps mentioned above but may require re-ordering of the steps. For example, if a major problem is found, then code may be released before being verified in the staging environment. In this case, a full set of tests would be performed in the staging environment after the problem is fixed in production.

## Front End Dependency Upgrade Policy

---

### Overview and Scope

Rethink uses the npm package management system via yarn, which is the world's largest software registry. We have two sets of packages, one for web and another for native applications (iOS and Android). In both cases, we are heavily dependent on the JavaScript ecosystem, which has a reputation for very large numbers of packages and dependencies when compared to other development environments.

### Rationale

There are several important reasons to stay up to date with JavaScript dependencies. The most important reason for our team is to prevent falling behind in features and bug fixes. Because we are dependent on the community to maintain our dependencies, and we use community documentation to develop features and fix bugs, it's very helpful to remain in sync with the community. Security is another compelling reason to stay current, as security issues are routinely reported and fixed by the community. Additionally, we recognize that dependency upgrades are unpredictable, and the complexity and time-risk of upgrading grows the longer upgrades are deferred.

### Process

To address these concerns, dependencies shall be evaluated and upgraded where possible every 90 days or less. We should use this process every other sprint to reduce the size of the upgrade task. In



the case of a security audit discovering a critical issue, this process should occur before the next release is finalized. Our current process is as follows, and applies to both web and native packages:

- Run `yarn upgrade-interactive --latest` to identify packages for upgrades
- Upgrade react-native with react-native upgrade as the docs say:  
<https://facebook.github.io/react-native/docs/upgrading.html>
- Upgrade dev Dependencies (these are lower risk, as they're only used by developers)
- Upgrade regular dependencies (these are higher risk, as they're used in production)

As dependencies are upgraded, commits should be made in the smallest unit possible, to allow for easy bisection later if an upgrade has caused a bug.

The git commit history shall serve as a record of this upgrade process. A ticket shall also be logged in JIRA to track the work of performing the process.

## Exclusions and forked packages

Some dependencies may need to be held back. Reasons for this include version incompatibility, introduction of bugs, or extensive development effort to complete the upgrade.

Additionally, some packages may be forked by the Rethink team to make patches. In these cases, our fork should bring in upstream changes where possible.

## Examples

Below are example scripts that may be helpful in this process, but will require manual intervention:

### For dev dependencies:

```
for pkg in $(yarn outdated --json | jq -js '[1].data.body | .[] | select(.[4]=="devDependencies") | "\(.[0])@\(.[3])"'); do yarn add "$pkg" --dev && git add package.json yarn.lock && git commit -m "Upgrade $pkg"; done
```

### For regular dependencies:

```
for pkg in $(yarn outdated --json | jq -js '[1].data.body | .[] | select(.[4]=="dependencies") | "\(.[0])@\(.[3])"'); do yarn add "$pkg" && git add package.json yarn.lock && git commit -m "Upgrade $pkg"; done
```

### If errors are found with failing tests, this snippet could be used to find the offending commit:

```
git bisect start && git bisect bad && git bisect good origin/develop git bisect run sh -c 'yarn && yarn test'
```

## Employee On-Call Policy

---

### Overview

The Employee On-Call Policy defines employee eligibility, the schedule, the duties of the person on call, and how to perform said duties. This policy should be reviewed and updated during the first week of every quarter.

### Eligibility

All employees that commit code to a codebase that is released to the production environment will be included in the On-Call Schedule.

### Schedule

Eligible employees will be on call every N weeks, where N equals the number of eligible employees. On-call shifts start on Friday at 5pm PST, and end at 8am PST Monday morning. If an employee is unable to cover their shift, switching with another eligible employee is allowed. If a modification to the schedule is needed, PagerDuty will need to be updated accordingly.

### Guidelines

While an employee is on call, he or she is not required to perform his or her normal duties. Rather, the employee is only responsible to respond if a situation occurs. Each eligible employee will have PagerDuty installed on his or her phone, which will send alerts to the appropriate person based upon the PagerDuty schedule.

### Escalation

During an event, the following escalation policy should be adhered to:

- Respond to the alert immediately and evaluate if the Rethink product is available for customers to use.
  - If not, a maximum of 5 minutes should be utilized to troubleshoot the problem before contacting a larger group. The individual should be capable of knowing who to contact based upon system behavior, and logging in Kibana.
  - If available, continue the investigation past the 5-minute barrier, and assess the risk associated with leaving the platform in its current state until Monday morning.
- If the current state is stable, a notification should be sent to the engineering group on Slack describing the problem, and that the decision was made to continue as-is until Monday morning.
- If, at any time, the on-call employee is not comfortable with the situation, or doesn't know how to proceed, their direct manager or VP of Engineering should be contacted to facilitate the situation.

## Background Check Policy

---

### PURPOSE OF BACKGROUND CHECK:

Rethink believes that hiring qualified individuals to fill positions contributes to the overall strategic success of Rethink. Background checks and reference checks serve as an important part of the selection process at Rethink. When a background check or reference check is needed with respect to hiring or other employment decisions, the company conducts such checks in compliance with applicable federal, state, and local laws.

This type of information is collected as a means of promoting a safe work environment for current and future Rethink employees. Background checks also help Rethink obtain additional applicant related information that helps determine the applicant's overall employability, ensuring the protection of the current people, property, and information of the organization. All offers of employment at Rethink are contingent upon clear results of a thorough background check.

### POLICY:

Reference checks are conducted on job applicants applying for all positions. Rethink will use a third-party agency to conduct background checks. The type of information that can be collected by this agency includes, but is not limited to, that pertaining to an individual's past employment, education, character, finances, reputation, etc. This process is conducted to verify the accuracy of the information provided by the applicant.

Rethink conducts background checks in compliance with applicable federal and state laws, including the Fair Credit Reporting Act, the California Investigative Consumer Reporting Agencies Act, and the California Consumer Credit Reporting Agencies Act. For example, the Americans with Disabilities Act prohibits organizations from collecting non-job-related information from previous employers or other sources. Therefore, the only information that can be collected is that pertaining to the quality and quantity of work performed by the applicant, the applicant's attendance record, education, and other issues that can impact the workplace. In addition, the procedure for background checks is such:

1. Applicants or employees will be provided with appropriate written notice of the company's intention to obtain information by way of a background check and will give applicants and employees the opportunity to obtain a free copy of any report obtained.
2. Applicants and employees will be asked to authorize a background check before such check is performed.

Background checks will include:

- **Social Security Verification:** validates the applicant's Social Security number, date of birth and former addresses.
- **Prior Employment Verification:** confirms applicant's employment with the listed companies, including dates of employment, position held and additional information available pertaining to performance rating, reason for departure and eligibility for rehire. This verification will be run on the past two employers or the previous five years, whichever comes first.



- **Personal and Professional References:** calls will be placed to individuals listed as references by the applicant.
- **Educational Verification:** confirms the applicant's claimed educational institution, including the years attended and the degree/diploma received.
- **Criminal History:** includes review of criminal convictions and probation. The following factors will be considered for applicants with a criminal history:
  - The nature of the crime and its relationship to the position.
  - The time since the conviction.
  - The number (if more than one) of convictions.
  - Whether hiring, transferring, or promoting the applicant would pose an unreasonable risk to the business, its employees or its customers and vendors.

The following additional background searches will be required if applicable to the position:

- **Motor Vehicle Records:** provides a report on an individual's driving history in the state requested. This search will be run when driving is an essential requirement of the position.
- **Credit History:** confirms candidate's credit history. This search will be run for positions that involve management of Rethink's funds and/or handling of cash or credit cards.
- Rethink can collect consumer credit information on applicants consistent with the guidelines set forth by the Federal Credit Reporting Act (FCRA). The Fair Credit Reporting Act requires organizations to obtain a candidate's written authorization before obtaining a credit report. Rethink obtains consumer credit reports only under very limited circumstances, for example, when applicants or employees are being considered for a management position in which they will have access to bank or credit card account information. When doing this, the employer must:
  - Certify to the consumer-reporting agency that the employer is in compliance with the FCRA and will not misuse the information it receives.
  - Disclosed to the applicant or employee, on a separate form, its plans to obtain a consumer or investigative consumer report and that the information received will be used solely for employment purposes.
  - Obtain written authorization from the applicant or employee.
  - Inform the individual of his or her right to request additional information on the nature of the report and the means through which such information may be obtained.
  - Inform the applicant that the report will include information about the individual's character, general reputation, personal characteristics, etc.
  - Provide the individual with a summary of his or her rights under the FCRA.
  - If the results of the credit check are negative, the organization must inform the applicant that it plans on taking adverse action, provide the applicant with a Statement of Consumer Rights from the FTC before adverse action, provide the applicant the opportunity to review a copy of their credit report, and advise the applicant of their rights to dispute inaccurate information. Applicants should be granted reasonable time to contest the information (approximately 3-5 days).

## RECORDKEEPING:

Rethink guarantees that all information obtained from the reference and background check process will only be used as part of the employment process and kept strictly confidential, in accordance with applicable legal requirements; and may only be reviewed or accessed by authorized individuals with the approval of HR. Human resources will maintain a log that will include the position you are applying for, your name, and the date of the background check. Be aware, only appropriate human resource personnel will have access to this information.

## Log Management Policy

---

### Purpose

The purpose of this policy is to establish a requirement to enable and review logs of Rethink apps and services.

### Scope

This policy covers all Rethink logs which are available currently, or which may be created, used in the future. This policy applies to all individuals who review and maintain the logs.

### Policy

Rethink apps and services logs are classified as Confidential or Private shall be electronically logged. Logging shall include all activity by Rethink's applications and service whenever available or deemed necessary. All logs are categorized as follows...

**DEBUG** Information relevant to programmers and system developers

**INFO** Information that describes operational events

**WARN** Information indicating a dangerous condition

**ERROR** Information that describes an application or system error

**FATAL** Information that a catastrophic state exists

### Review Policy

Log activity review cycles shall include review of audit logs minimally every 30 days and may include weekly exception reporting.





## Rethink Member Acknowledgement

---

**Rethink Privacy Officers:**

Robert Johnson, General Counsel

**Executive Contact:**

Eran Rosenthal, President and COO

Confirmation

I have received a copy of the Rethink Information Security Policies as part of my training. My signature below indicates I have read the policies and understood both Rethink's responsibilities as well as my personal responsibilities.

\_\_\_\_\_  
Employee Name

\_\_\_\_\_  
Date

\_\_\_\_\_  
Rethink Inc. Management

\_\_\_\_\_  
Date

# RethinkAutismInc\_Erie1BOCES\_NY\_Add-On\_VendorSigned

Final Audit Report

2025-06-03

Created:	2025-06-02
By:	Keith Perham (kperham@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAACLA7SUO0HXnEPczTr_TPFtK3qgb_Pfsp

## "RethinkAutismInc\_Erie1BOCES\_NY\_Add-On\_VendorSigned" History

-  Document created by Keith Perham (kperham@tec-coop.org)  
2025-06-02 - 5:34:41 PM GMT
-  Document emailed to James Fregelette (jfregelette@e1b.org) for signature  
2025-06-02 - 5:36:15 PM GMT
-  Email viewed by James Fregelette (jfregelette@e1b.org)  
2025-06-02 - 6:06:13 PM GMT
-  Document e-signed by James Fregelette (jfregelette@e1b.org)  
Signature Date: 2025-06-03 - 3:37:38 PM GMT - Time Source: server
-  Agreement completed.  
2025-06-03 - 3:37:38 PM GMT