BROOME•TIOGA boces
Enriching Lives Through Education

Broome-Tioga BOCES
Parents' Bill of Rights for Data Privacy and Security

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

- A student's personally identifiable information cannot be sold or released for any commercial purposes.
- Parents have the right to inspect and review the complete contents of their child's education record.
- State and federal laws protect the confidentiality of personally identifiable information and safeguards associated with industry standards and best practices, including, but not limited to, encryption, firewalls, and password protection must be in place when data is stored or transferred.
- A complete list of all student data elements collected by the state is available for public review at http://www.nysed.gov/data-privacy-security/student-data-inventory, or by writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
- Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY, 12234. Complaints may also be directed to the Chief Privacy Officer via email at: privacy@nysed.gov.
- The BOCES will promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect personally identifiable information.

Appendix
Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services, Broome-Tioga BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data" as those terms are defined by law.

Each contract BOCES enters into with a third-party contractor, where the third-party contractor receives student data or teacher or principal data, will include the following information:

- The exclusive purposes for which the student data or teacher or principal data will be used.
- How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements.
- When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement.
- If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected.
- Where the student, teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

This section to be completed by the Third-Party Contractor and returned to Broome-Tioga BOCES

Section 1: Does the Third-Party Contractor have access to student data and/or teacher or principal data as those terms are defined by law?

X Yes
Please complete Sections 2, 3 and 4

□No
Please complete Section 3

Section 2: Supplemental Information Details
Third-Party Contractors subject to New York Education Law § 2-d – please complete the table below

SUPPLEMENTAL INFORMATION ELEMENT	SUPPLEMENTAL INFORMATION
Please list the exclusive purpose(s) for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract (or list the section(s) in the contract where this information can be found)	Rubrik products and services will be used by Customer to back up their data. Rubrik will not use Customer data for any purpose other than as reasonably necessary for Rubrik to provide the Rubrik Service to Customer. Customer is the Data Controller and Rubrik is a Data Processor.
Please list how the contractor will ensure that any other entities with which it shares the protected data, if any, will comply with the data protection and security provisions of law, regulation and this contract (or list the section(s) in the contract where this information can be found)	Rubrik evaluates all suppliers & subcontractors through an established supplier security risk management program. Suppliers are reviewed through Rubrik's Procurement and Supplier Security process, which assesses suppliers based on the criticality of the services they provide. Suppliers are reviewed on an annual basis, and are evaluated for adherence to standards and terms.
Please list when the agreement expires and what happens to the protected data when the agreement expires (or list the section(s) in the contract where this information can be found)	The agreement expires when the last Subscription Period expires. Rubrik will help to extract the data to customer's location choice. For hosted SaaS, customer can remove or retrieve data from the provision in the case of an early termination or non-renewal of the contract for up to 30 days after expiration or termination.
Please list how a parent, student, or eligible student may challenge the accuracy of the protected data that is collected; if they can challenge the accuracy of the data, describe how (or list the section(s) in the contract where this information can be found)	Rubrik is not responsible for accuracy of Customer data. Customer is the Data Controller, and Rubrik is the Data Processor.
Please list where the protected data will be stored (described in a way that protects data security), and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated (or list the section(s) in the contract where this information can be found)	Customer will be able to choose the data backup location during setup. Kindly refer to Rubrik's standard commercial terms and Customer Data Security Schedule and Data Processing Addendum on Rubrik's website that Rubrik offers to all customers.
Please list how the data will be protected using encryption (or list the section(s) in the contract where this information can be found)	RSC uses AES-256 for data at-rest and data in-flight encryption. All critical customer configuration information is encrypted using modern cryptography via Google Managed Encryption Keys. Sensitive fields in the database are encrypted using an encryption framework built on top of GCP's Cloud Key Management Service and Cloud IAM. A key management process is in place to facilitate key rotation and revocation. All backup data is encrypted using the AES 256-bit algorithm. All communications with Rubrik UI and APIs are encrypted via industry standard HTTPS/TLS (TLS 1.2+) over public networks.

Section 3: Agreement and Signature

By signing below, you agree:

- The information provided in this document by the Third-Party Contractor is accurate
- To comply with the above terms of Broome-Tioga BOCES Parents' Bill of Rights for Data Privacy and Security (applicable to Third-Party Contractors subject to New York Education Law § 2-d only) identified in bullets on page 1 of this document.

Company Name Rubrik, Inc. Product Name Rubrik Cloud Vault

Printed Name Anne-Marie Eileraas Signature DocuSigned by: Anne-Marie Eileraas 376BA595A7D34BC... Date Aug 1, 2023 | 10:05 PM PDT

Section 4: Data Privacy Rider for All Contracts Involving Protected Data Pursuant to New York State Education Law §2-C and §2-D

BOCES and the Third-Party Contractor agree as follows:

1. Definitions:
   a. Protected Information means personally identifiable information of students from student education records as defined by FERPA, as well as teacher and Principal data regarding annual professional performance reviews made confidential under New York Education Law §3012-c and §3012-d;
   b. Personally Identifiable Information (PII) means the same as defined by the regulations implementing FERPA (20 USC §1232-g);

2. Confidentiality of all Protected Information shall be maintained in accordance with State and Federal Law and the privacy and security requirements found in Rubrik's standard commercial terms offered to all customers in the Rubrik Customer Data Security Schedule and Rubrik Data Processing Addendum on Rubrik's website at this location: https://www.rubrik.com/legal;

3. The Parties agree that the BOCES's Parents' Bill of Rights for Data Security and Privacy identified in bullets on page 1 of this document, are incorporated as part of this agreement, and the Third-Party Contractor shall comply with its terms;

4. The Third-Party Contractor agrees to comply with New York State Education Law §2-d and its implementing regulations;

5. The Third-Party Contractor agrees that any officers or employees of the Third -Party Contractor, and its assignees who have access to Protected Information, have received or will receive training on Federal and State law governing confidentiality of such information prior to receiving access;

6. The Third-Party Contractor shall:
   a. limit internal access to education records to those individuals that are determined to have legitimate educational interests;
   b. not use the education records for any other purposes than those explicitly authorized in its contract or written agreement. Unauthorized use specifically includes, but is not limited to, selling or disclosing personally identifiable information for marketing or commercial purposes or permitting, facilitating, or disclosing such information to another Third-Party for marketing or commercial purposes;
   c. except for authorized representatives of the Third-Party Contractor to the extent they are carrying out the contract or written agreement, not disclose any personally identifiable information to any other party;
      i. without the prior written consent of the parent or eligible student; or
      ii. unless required by statute or court order and the party provides notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by statute or court order;
   d. maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
   e. use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the Secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law §111-5;
   f. adopt technology, safeguards and practices that align with the NIST Cybersecurity Framework;
   g. impose obligations consistent with those found in this rider in writing where the Third -Party Contractor engages a subcontractor or other party to perform any of its contractual obligations which provides access to Protected Information.

Agreement and Signature

By signing below, you agree to the Terms and Conditions in this Rider:

Company Name Rubrik, Inc. Product Name Rubrik Cloud Vault

Printed Name Anne-Marie Eileraas Signature DocuSigned by: Anne-Marie Eileraas 376BA595A7D34BC... Date Aug 1, 2023 | 10:05 PM PDT