EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

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

1. **Purpose**

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

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

2. **Definitions**

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

In addition, as used in this Exhibit:

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

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

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

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

3. **Confidentiality of Protected Data**

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

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy.. Erie 1 BOCES will provide Vendor with a copy of its policy. Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

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

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

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

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA: [Insert here – also provide a copy of Data Security and Privacy Plan]

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	LinkIt! maintains strict privacy and security protocols that are established in accordance with industry standards. These include both technical safeguards and procedural safeguard with respect to data access and sharing procedures. More details on our plan may be found online at: https://www.linkit.com/privacy-policy
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	The safeguards in place to protect PII data are too numerous to fully detail here, but data and files are stored securely on the industry-leading Amazon (AWS) hosting platform. Our data and security model follows best practices and consists principally of the following: • **Physical Security:** Web servers, data servers and network data storage are on servers maintained by AWS. We perform full daily backups and hourly incremental backups which are stored offsite in the event of a disaster. The data center is located in a secure area with restricted onsite access. • **Data Security:** LinkIt! utilizes industry-leading Microsoft SQL database that enables encryption in transit and at rest. Electronic access to database servers is restricted through dedicated web servers on a local network. This provides an effective barrier against attempts to directly compromise database integrity. • **Web Security:** Our web layer consists of a passcode encrypted web service with enforced business logic. The business logic restricts user activity based upon permission level such that data access is limited to role within the LEA organization.

3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Our employees undergo annual training related to data handling and privacy/security issues. This includes protocols for sharing PII data, requiring it to be sent via a secure method, such as SFTP, instead of via email. Employees are also trained to avoid printing documents with PII unless required to do so and to refrain from sharing data with any person outside of their designated contact at the school or district or others that are explicitly authorized to receive such data.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	All employees and subcontractors sign a NDA related to data handling. Any breach of this agreement is grounds for termination and the offending party may also risk criminal prosecution and civil penalties as a result.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Details on the policies and procedures related to PII handling may be found here, but LinkIt! is committed to prompt notification of any breaches within seven (7) days after initial discovery. The company also performs internal scans to detect such breaches (or attempts) as well as regular penetration and vulnerability testing via a third party firm to identify and mitigate potential risks and vulnerabilities.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Data will be transitioned to EA within 7 days of receipt of written request for the same, or, in the absence of such notice, within 60 days of termination of contract. A copy of the data set may also be provided to authorized EA staff upon request following the termination of the Agreement.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Written certification of the data destruction is provided on a notarized form signed by a member of the company's senior executive team and provided upon request of the EA.

8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Our data and security guidelines have been developed to reflect the current NYS guidelines and frameworks, including but not limited to the Parents Bill of Rights.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	*LinkIt! has well defined data handling and operational protocols that are appropriate to meet the needs of the organization and its clients as it pertains to risk mitigation and planning purposes. The company has also implemented a company-wide device management system to lower the risk of unauthorized access to our data systems.*
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	*LinkIt! has established a culture and operational model that prioritizes privacy and data security. The company is entirely focused on enabling educational agencies to make better decisions using their data, including PII, so the relative importance of security and privacy are firmly ingrained in all aspects of company mission, policies and procedures and activities across the various roles and areas of responsibility.*
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	*LinkIt! has an experienced executive team and employees industry experts on a consultative basis to establish, manage, and monitor risk as it pertains to compliance mandates and operational protocols. The challenges and potential risks from a privacy/security standpoint are well-known to all company stakeholders and reinforced through ongoing training and other initiatives.*
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	*Within LinkIt!, cybersecurity risks are well-known and both staff and management are aware of the gravity and potential reputational consequences of a data breach or similar event in which PII data becomes exposed. These risks are mitigated in a variety of ways, including legal agreements, operational practices, third party compliance tools, and ongoing awareness training.*
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Risk management with respect to the protection of PII is always a mission-critical company priority. Given that LinkIt! has no other business lines (i.e. various divisions competing for access to resources), the collection, management and analysis of sensitive data is always of paramount importance and is not compromised. We therefore maintain an extremely conservative approach with respect to risk tolerance when it comes to data security practices.

Function	Category	Contractor Response
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	*LinkIt! relies on only highly established industry-leading vendors, such as Microsoft and AWS (Amazon Web Services) to deliver the backbone of our physical and logical security measures. Purchasing and/or licensing solutions from only a limited number of such vendors enables us to mitigate supply chain risk and evaluation of incremental risk factors are always of critical importance when decisions are made to expand the company's ecosystem of suppliers.*
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	*Physical and logical assets are housed in secure data centers managed by industry leader Amazon Web Services. The specific locations of these facilities are not disclosed to the public and are highly secure. LinkIt! company offices where company devices are stored are also secured with keyed elevator access and are not accessible to any individual that has not been granted keyed access.*
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	*LinkIt! employees receive annual training in security and privacy best practices and general awareness in addition to role-related data-handling training protocols. This level of sensitivity to appropriate handling of PII data is critical to daily operations and company culture.*
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	*LinkIt! manages data in a manner that is consistent with the sensitivity thereof and has established data retention (and destruction) protocols to ensure that such data is purged from company servers at the request of client EA's or at the conclusion of a contract term. Access to such data is also restricted to those individuals and roles requiring such access in order to perform their support and service responsibilities.*
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	*LinkIt! has established numerous security procedures and protocols that define how data is to be managed and shared within and across internal and external stakeholder groups, including policies related to data encryption requirements and two-factor authentication for systems and device access.*

Function	Category	Contractor Response
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	*Maintenance, including the implementation of recommended security patches, are performed on a regular basis in accordance with industry best practices.*
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	*LinkIt! uses a variety of technical solutions to promote system security and resilience. The majority of such solutions are managed by AWS and Microsoft.*
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	*Advanced monitoring systems are in place to detect unusual activity, including attempted data breaches and DOS attacks. The company also undergoes periodic 3rd party penetration testing in order to identify and ameliorate potential vulnerabilities.*
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	*As noted above, LinkIt! uses 3rd party security solutions from industry leading partners to monitor potential cybersecurity events, including Microsoft Defender for Endpoint.*
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	*LinkIt! has established policies and procedures in order to identify anomalous events. These procedures are aided by third party tools, including Microsoft Defender for Endpoint, as noted above.*
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	*LinkIt! has established thorough disaster recovery procedures and has tested these procedures to establish recovery benchmarks. The company intends to perform complete disaster response and recovery tests at least once every 24 months and document the same.*
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	*The LinkIt! response plan involves coordination with applicable enforcement agencies as appropriate based upon the nature of the incident.*
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	*LinkIt! has established thoughtful and effective response and recovery procedures, inclusive of communication guidelines that*

Function	Category	Contractor Response
		have been refined and improved over time. The company maintains a real-time status/availability page and can notify impacted clients at scale in the event that such notification is appropriate.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	*The principle of containment is always front and center with respect to any ongoing incident. Though specific actions may vary based on the severity and nature of the incident, the first actions taken after identification relate to the mitigation and can include protocols such as taking the database or web servers offline entirely pending further investigation and review.*
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	*LinkIt! has made numerous updates to its security incident response practices and procedures in response to both operational experience, internal testing and 3rd party review/recommendations. Such changes have been implemented in order to mitigate potential risks identified through testing and actual operational experience.*
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	*The LinkIt! technical operations team is well versed in backend infrastructure architecture and has practiced both partial and full system recovery following simulated incidents. Such recovery protocols always emphasize data asset protection and we work to restore any data that may have been corrupted or lost via secure backup sources.*
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	*Like response practices, recovery practices are also informed by operational experience, including results of periodic testing to establish benchmarks for systems recovery timelines and related matters. While minimizing system downtime is a key priority, it is secondary in nature to data privacy/integrity considerations.*
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	*Restoration activities are always coordinated with internal and external parties under the direction of the company CTO/CIO. While the specifics of the communications vary based upon incident circumstances, keeping all stakeholders informed regarding the incident's status is a critical priority.*

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

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

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

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

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

5. **Additional Statutory and Regulatory Obligations**

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

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

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

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

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

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

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

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

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

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

6. **Notification of Breach and Unauthorized Release**

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

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

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

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

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

EXHIBIT D (CONTINUED)

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

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

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available for public review at **http://www.nysed.gov/data-privacy-security/student-data-inventory**, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website **http://www.nysed.gov/data-privacy-security/report-improper-disclosure**.

BY THE VENDOR:

Signature DocuSigned by: Daniel Gross 6AF2B983A869408...

Printed Name Daniel Gross

Title NY Account Director

Date 5/6/2023

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND [LINKIT!]

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with [LinkIt!] which governs the availability to Participating Educational Agencies of the following Product(s):

[LinkIt! Climate Survey Application]

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

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

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: *Vendors that receive PII will address statutory and regulatory data privacy and security requirements. Additional information on subscontractors can be found in "Supply Chain Risk Management" section of the Data Security and Privacy Plan on page 23.*

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on July 1, 2023 and expires on June 30, 2026.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

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

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

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