

# NEW YORK STATE MODEL DATA PRIVACY AGREEMENT FOR EDUCATIONAL AGENCIES

**Letchworth Central School District**

**and**

**Advanced Assessment Systems d/b/a LinkIt!**

This Data Privacy Agreement ("DPA") is by and between the Letchworth Central School District ("EA"), an Educational Agency, and LinkIt! ("Contractor"), collectively, the "Parties".

## ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, 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.

8. **NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal 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.

## ARTICLE II: PRIVACY AND SECURITY OF PII

### 1. Compliance with Law.

In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated 27 March 2025 ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law.

Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

**2. Authorized Use.**

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

**3. Data Security and Privacy Plan.**

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

**4. EA's Data Security and Privacy Policy**

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

**5. Right of Review and Audit.**

Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

**6. Contractor's Employees and Subcontractors.**

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
- (e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

#### **7. Training.**

Contractor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

#### **8. Termination**

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

#### **9. Data Return and Destruction of Data.**

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.
- (b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.
- (c) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

#### **10. Commercial or Marketing Use Prohibition.**

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

#### **11. Encryption.**

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

**12. Breach.**

(a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address:

John P. Novak

Data Protection Officer, Letchworth CSD

5550 School Road

Gainesville, NY 14066

jnovak@letchworth.k12.ny.us

**13. Cooperation with Investigations.**

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

**14. Notification to Individuals.**

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

**15. Termination.**

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

### **ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS**

**1. Parent and Eligible Student Access.**

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

**2. Bill of Rights for Data Privacy and Security.**

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.


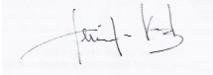
### **ARTICLE IV: MISCELLANEOUS**

**1. Priority of Agreements and Precedence.**

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

## 2. Execution.

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

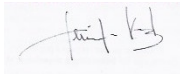
EDUCATIONAL AGENCY	CONTRACTOR
BY: 	BY: 
<b>John P. Novak</b>	<b>Jennifer Kurtz</b>
<b>Data Protection Officer</b>	<b>Chief Information Security Officer, LinkIt!</b>
Date: 4/2/25	Date: 03/27/2025



## EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at [www.nysed.gov/data-privacy-security/student-data-inventory](http://www.nysed.gov/data-privacy-security/student-data-inventory) and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted using the [Letchworth CSD Complaint Form](#) or to the District's Data Protection Officer, John P. Novak, by mail to: Letchworth CSD, 5550 School Road, Gainesville, NY 14066, by email to [jnovak@letchworth.k12.ny.us](mailto:jnovak@letchworth.k12.ny.us), or by telephone to 585-493-5150. (ii) Complaints may also be submitted to the NYS Education Department at [www.nysed.gov/data-privacy-security/report-improper-disclosure](http://www.nysed.gov/data-privacy-security/report-improper-disclosure), by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to [privacy@nysed.gov](mailto:privacy@nysed.gov); or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	
[Printed Name]	Jennifer Kurtz
[Title]	Chief Information Security Officer, LinkIt!

Date:

3/27/2025

## EXHIBIT B

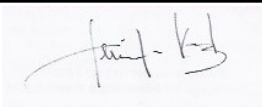
## BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -

## SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

<b>Name of Contractor</b>	<b>Advanced Assessment Systems d/b/a LinkIt!</b>
<b>Description of the purpose(s) for which Contractor will receive/access PII</b>	The exclusive purposes for which "student data" or "teacher or principal data" (as those terms are defined in Education Law Section 2-d and collectively referred to as the "Confidential Data") will be used by LinkIt! (the "Contractor") are limited to the purposes authorized in the contract between the Contractor and Letchworth Central School District (the "EA") dated 3/27/2025 (the "Contract").
<b>Type of PII that Contractor will receive/access</b>	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> APPR Data (optional: as determined by LEA)
<b>Contract Term</b>	Contract Start Date <u>3/27/2025</u> Contract End Date _____
<b>Subcontractor Written Agreement Requirement</b>	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" type="checkbox"/> Contractor will utilize subcontractors.
<b>Data Transition and Secure Destruction</b>	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> <li>• Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties.</li> <li>• Securely delete and destroy data.</li> </ul>
<b>Challenges to Data Accuracy</b>	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the

	EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
<b>Secure Storage and Data Security</b>	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p> <p>Confidential Data provided to Contractor by the EA will be encrypted and stored in a SOC-compliant, secured, AWS data facility that is monitored 24/7 and located within the US. The measures that Contractor takes to protect Confidential Data align with the NIST Cybersecurity Framework including, but not necessarily limited to, disk encryption, file encryption, firewalls, access control mechanisms, boundary protection, and secure network and database architecture.</p>
<b>Encryption</b>	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	
[Printed Name]	Jennifer Kurtz
[Title]	Chief Information Security Officer, LinkIt!
Date:	3/27/2025

## EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

### CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	<p>LinkIt! maintains strict privacy and security protocols that are established in accordance with industry standards, the NIST CSF 2.0 and other frameworks (i.e., ISO/IEC 27001, NIST SP 800-171r3, CISv8, and CMMC Level 1). These protocols and mechanisms include technical, physical, and procedural or administrative safeguards with respect to safely and securely handling protected data. More details on our plan may be found online at: <a href="https://www.linkit.com/privacy-policy">https://www.linkit.com/privacy-policy</a>. The control areas implemented align with NIST SP 800-171r3:</p> <ul style="list-style-type: none"><li>3.1 Access Control (AC)</li><li>3.2 Awareness and Training (AT)</li><li>3.3 Audit and Accountability (AU)</li><li>3.4 Configuration Management (CM)</li><li>3.5 Identification and Authentication (IA)</li><li>3.6 Incident Response (IR)</li><li>3.7 Maintenance (MA)</li><li>3.8 Media Protection (MP)</li><li>3.9 Personnel Security (PS)</li><li>3.10 Physical Protection (PE)</li><li>3.11 Risk Assessment (RA)</li><li>3.12 Security Assessment and Monitoring (CA)</li><li>3.13 Systems and Communication Protection (SC)</li><li>3.14 System and Information Integrity (SI)</li><li>3.15 Planning (PL)</li><li>3.16 Systems and Services Acquisitions (SA)</li><li>3.17 Supply Chain Risk Management</li></ul> <p>Our Data Privacy and Security Plan is available upon request. LinkIt reviews and updates that plan annually to ensure continued alignment with federal, state, and local requirements.</p>
---	--	---

2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	<p>LinkIt has implemented numerous administrative, operational, and technical safeguards and practices to protect PII. These safeguards conform to those in CISv8 and the 17 control families described in NIST SP 800-171r3. Our data and security model also follow the well-architected AWS framework and the functions outlined in the NIST Cybersecurity Framework (CSF 2.0).</p> <p>Safeguards include the following:</p> <p><b>Administrative Controls.</b> LinkIt! implemented policies and plans related to security and privacy as part of its initiative to achieve ISO/IEC compliance in 2016. Since 2022, those policies and plans have been reviewed annually and updated as appropriate. Employees and subcontractors receive training on their provisions, which include the following: Acceptable Use Policy (aka Information Security Policy), Customer Platform Account Management Policy, Data Security and Privacy Plan, Incident Response Plan, Operations Security Guidelines, Privacy Policy, Systems Administration and Configuration Policy, and (recently drafted) Vulnerability Disclosure Policy</p> <p><b>Communications Security.</b> LinkIt encrypts communications among remote team members and software development team members using VPN as appropriate.</p> <p><b>Data Security.</b> LinkIt! utilizes industry-leading Microsoft SQL database that enables encryption in transit and at rest in accordance with the technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5 (e.g., SHA 256). As described above, the digital infrastructure is maintained in a locked facility. Both that facility and system activity are monitored 24/7. Anomalies are flagged, addressed, logged, and escalated for further resolution as</p>
---	---	--

		<p>appropriate. Electronic access to database servers is restricted through dedicated web servers on a local network. MFA is implemented for access to network resources. This provides an effective barrier against attempts to compromise database integrity directly. Only encrypted PII is transmitted to authenticated and authorized users.</p> <p><b>Network and Device Security.</b> LinkIt has implemented firewall and anti-malware protections on all corporate-owned devices. Default passwords have been deactivated and secure configurations have been implemented. Network activity is monitored 24/7. LinkIt uses safelisting mechanisms to reduce the risk of malicious attacks. Users authenticate to network resources using MFA or 2FA with more granular controls (e.g., attribute-based and role-based access controls). The network is segmented to enforce least privilege and least functionality.</p> <p><b>Personnel and Process Security:</b> Our employees undergo quarterly training (at a minimum) related to data handling and privacy/security issues. This includes updates on federal and state privacy regulations and required protocols for sharing PII data (e.g., requiring it to be sent via a secure method, such as SFTP, instead of via email). Employees are 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. Employees report phishing attempts to the CISO who recommends further action as needed.</p> <p><b>Physical Security.</b> Web servers, data servers and network data storage are maintained by a SOC2-compliant cloud services provider in a locked data center with restricted onsite access and located within the United States. LinkIt performs full backups</p>
--	--	--

		<p>weekly, differential backups daily, and incremental transactional backups every ten minutes. Local backups are stored on disk, in addition to being stored securely with AWS S3 (cloud storage service). Access to LinkIt headquarters is restricted to known staff members. Any media containing PII is locked up. Access to server rooms and media storage areas is controlled.</p> <p><b>Platform Security.</b> Our platform consists of a passcode-encrypted web service with enforced business logic. The business logic restricts user activity based upon permission levels specified by the LEA that limits data access according to the user's role within the LEA organization. All system activity is monitored, logged, and flagged for anomalies 24/7. The Cybersecurity and Infrastructure Security Agency (CISA), an agency of the US Department of Homeland Security, performs a minimum of monthly vulnerability assessments on the LinkIt platform. Any findings are resolved immediately by LinkIt IT team members.</p> <p><b>Secure Software Development.</b> LinkIt has implemented controls to isolate testing and development environments from production environments. All sensitive data is anonymized/masked in non-production environments. Non-production environments (e.g., those for development or testing) are protected by the same level of security controls as production (live) environments. LinkIt has signed the Secure by Design Pledge &lt;<a href="https://www.cisa.gov/k-12-education-technology-secure-design-pledge">https://www.cisa.gov/k-12-education-technology-secure-design-pledge</a>&gt; and is in the process of fully implementing its principles and best practices for K-12 education technology.</p> <p><b>Third-Party Risk</b> LinkIt staff and contractors are not permitted to store sensitive information on unauthorized, unencrypted devices (per LinkIt</p>
--	--	--

		Acceptable Use Policy). LinkIt contractors agree via signed contract to follow security protocols and disposal processes that align with LinkIt processes and the NIST SP 800-171 guidelines.
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.	Training on data security, privacy, and related federal, state, and local laws and regulations is part of our employee onboarding process. The training is revisited throughout the year as “cybersecurity briefs” during biweekly meetings and also when our employees undergo annual training related to data handling and privacy/security issues. Topics include protocols for sharing PII data securely, client interaction guidelines, phishing detection and reporting, minimal hard copy printing of documents with PII (unless required to do so by the LEA), secure destruction of PII-containing documents or media, MFA, and robust password practices.
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 LinkIt employees and subcontractors sign a NDA related to data handling. Any breach of this agreement is grounds for termination; the offending party may also risk criminal prosecution and civil penalties as a result. LinkIt uses third-party vendors that incorporate NIST SP 800-171 controls into their practices to provide the necessary security envelope for hosting and protecting the collection, processing, and storage of student- and educator-related data, as well as proprietary software code. Contractor compliance with LinkIt’s safe data-handling practices is contractually confirmed through signed supplier information security agreements. Such agreements are signed with suppliers that provide both platform development and client technical support services. These agreements are part of our shared responsibility model for maintaining the security of proprietary data and zones of trust. Communications with subcontracted software development



		<p>team members are secured via VPN.</p> <p>De-identified PII is not used in the development or testing environments.</p>
5	<p>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.</p>	<p>Additional details on the policies and procedures related to PII handling may be found <a href="#">here</a>, 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.</p> <p>Our Incident Response Plan is available upon written request.</p>
6	<p>Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.</p>	<p>LinkIt returns Student and/or Teacher or Principal data in a usable, protected, electronic format upon request from the contracting District or LEA after contract termination. Data is transmitted via Secure File Transfer Protocol (SFTP) or another secured transport mechanism as determined by the District. LinkIt now requires that a multiparty document be signed by LEAs to authorize that data be disclosed, transferred, or shared in accordance with FERPA provision 34 CFR §99.34. (This is the exception that allows such disclosure based on a student's enrollment status.)</p> <p>LinkIt's policy is to permanently erase, destroy, or otherwise render inaccessible or unrecoverable customer data within 60 days of service agreement termination and in accordance with NIST SP 800-88. As part of the AWS contracted services, virtual volumes are wiped before they are terminated with AWS according to its deletion process. Retention policies remove backups from the AWS Simple Storage Service (S3) cloud. LinkIt staff and contractors are not permitted to store sensitive information on unauthorized, unencrypted devices (per LinkIt Acceptable Use Policy). LinkIt contractors agree to follow secure disposal processes that align with LinkIt processes. Hard copies of documents containing protected information shall either</p>

		be returned via secure means to clients upon the termination of an engagement or shredded, as required by contract and laws governing client data and privacy protection. 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 LEA.
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. Data destruction practices follow NIST SP 800-88 recommendations.
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 and NYC 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.

## EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies ); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

Function	Category	Contractor Response
<b>IDENTIFY (ID)</b>	<b>Asset Management (ID.AM):</b> 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 for endpoint protection to lower the risk of unauthorized access to our data systems. Infrastructure

Function	Category	Contractor Response
		components are maintained and monitored 24/7 in a secured, SOC2-compliant facility operated within US boundaries by AWS. Internally, devices are patched regularly, as is anti-malware protection.
	<b>Business Environment (ID.BE):</b> 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. Senior management is fully engaged in maintaining the security, integrity, availability, and confidentiality of the data it handles. 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. This includes internal audits of business processes and relevant policies at least annually and monthly vulnerability assessments performed by CISA.
	<b>Governance (ID.GV):</b> 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 employs industry experts on a consultative basis to establish, manage, and monitor risk as it pertains to compliance mandates, legal and regulatory changes (federal, state, local), 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. Policies, procedures, and processes are reviewed and revised at least annually to ensure ongoing conformance to current and related NIST, CIS, and ISO/IEC frameworks.
	<b>Risk Assessment (ID.RA):</b> 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, functional, financial, and legal consequences of a data breach or similar event in which PII data is exposed or otherwise compromised. These risks are mitigated in a variety of ways, including legal agreements, operational practices, third-party technical tools for enforcement, and ongoing awareness training. LinkIt recently completed a self-assessment against the CISv8 guidelines. CISA performs vulnerability assessments at least monthly on the LinkIt web application. LinkIt is also in the process of performing a gap analysis against NIST SP 800-171r3 (the newest version), CSF 2.0, and the Cybersecurity Rubric for Education.
	<b>Risk Management Strategy (ID.RM):</b> 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 LinkIt priority. LinkIt's business is data and its safe and reliable collection, warehousing, maintenance, analysis, reporting, and use for informed decision-making by LEAs. We therefore maintain an extremely conservative approach with respect to risk tolerance when it comes to data security and privacy practices.
	<b>Supply Chain Risk Management (ID.SC):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk	LinkIt relies only on well-established and vetted industry-leading vendors, such as Microsoft and AWS (Amazon Web Services), to help manage and support its physical and logical security measures. Purchasing and/or licensing solutions from only a

Function	Category	Contractor Response
	decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	limited number of such vendors enables us to mitigate supply chain risk. Evaluation of incremental risk factors are always of critical importance when decisions are made to expand the company's ecosystem of suppliers. LinkIt requires that its third-party providers sign contracts that attest to their commitment to maintaining data confidentiality and security practices equivalent to, consistent with, and no less protective than, those found in this DPA. These data and privacy protection agreements with third-party service providers confirm their compliance with applicable state and federal laws and regulations. LinkIt also consults with US DOE's PTAC when questions arise about best practices viz a viz federal regulations.
PROTECT (PR)	<b>Identity Management, Authentication and Access Control (PR.AC):</b> 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 infrastructure assets are housed in secure data centers managed by SOC2-compliant, industry leader Amazon Web Services. These facilities are located in the United States (for domestic clients) and monitored 24/7. The specific locations of these facilities are not disclosed to the public and are highly secure. LinkIt company offices, in which company computing devices are stored, are also secured with keyed elevator access and are not accessible to any individual that has not been granted keyed access. Access to servers and locked cabinets is limited to a few individuals. MFA is in place to control access to network-based resources. VPN connections are required for remote access to database repositories. Such access is limited to specific individuals. System activity is monitored and logged 24/7 and audit logs are maintained. Least privilege, least functionality, and separation of duty principles guide role-based access control mechanisms.
	<b>Awareness and Training (PR.AT):</b> 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, at a minimum, quarterly training in security and privacy best practices, general awareness of current and emerging threats, and applicable state and federal laws/regulations, 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. Security awareness training is also included as part of the new-hire orientation process. LinkIt team members and development partners are briefed during all-hands meetings about real-world cybersecurity incidents within the K12 sector, phishing, and BEC attempts seen within LinkIt. Our internal and external team members are encouraged to report anomalous activities to the CISO for further action.

Function	Category	Contractor Response
	<b>Data Security (PR.DS):</b> 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 LEAs or at the conclusion of a contract term. These protocols follow NIST guidelines. Access to such data is also restricted to those individuals and roles requiring such access in order to perform their support and service responsibilities, in keeping with LinkIt's least privilege/least functionality philosophy. LinkIt has established a process for record validation and review, as well as a Customer Platform Account Management Policy. With respect to requests for the disposition of records (e.g., transfer, deletion, or sharing with another EA), LinkIt requests that a signed copy of either its multiparty form for authorizing access to the data or a similar document (like the form developed by the Student Data Privacy Consortium or SDPC) accompany the request. To ensure the availability of information, LinkIt performs full backups weekly, differential backups daily, and incremental transactional backups every ten minutes. Local backups are stored on disk, in addition to being stored securely with AWS S3 (cloud storage service).
	<b>Information Protection Processes and Procedures (PR.IP):</b> 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 implemented its information security management system (ISMS) with enforcing policies and procedures in 2016 as part of its ISO/IEC 27001 initiative. It updates these policies regularly to ensure their continued relevance as customer, legal/regulatory, business, threat, and technological conditions change. The NIST SP 800-171 initiative, launched in 2022, prompted implementation of additional policies and procedures to align with the NIST framework recommendations and define how data is to be managed and shared within and across internal and external stakeholder groups. LinkIt is also a signatory to the CISA <i>Secure by Design Pledge</i> , which has led to work on its vulnerability disclosure policy and additional steps in its software development practices.
	<b>Maintenance (PR.MA):</b> 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 and software updates, are performed on a regular basis in accordance with industry best practices. LinkIt does not use industrial control technologies.
	<b>Protective Technology (PR.PT):</b> 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 including endpoint and email security, data encryption, firewall protection, and secure network and database architecture. The LinkIt IT team coordinates with relevant third-party providers to manage these solutions. The CISO reviews proposed agreements with prospective partners (e.g., researchers, content providers) to control potential risks to protected data, systems, and intellectual property.
<b>DETECT (DE)</b>	<b>Anomalies and Events (DE.AE):</b> Anomalous activity is detected and the potential impact of events is understood.	Advanced, 24/7 monitoring systems with system activity logs are in place to detect unusual activity, including attempted data

Function	Category	Contractor Response
		breaches and DOS attacks. LinkIt's third-party service provider flags anomalies in the performance of infrastructure components and immediately addresses, mitigates, or escalates treatment to the LinkIt IT Team as appropriate. LinkIt also undergoes periodic third-party penetration testing in order to identify and mitigate potential vulnerabilities. LinkIt's incident response plan (IRP) follows the guidelines in NIST SP 800-61r2.
	<b>Security Continuous Monitoring (DE.CM):</b> The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	As noted above, LinkIt uses third-party security solutions from industry leading partners to monitor potential cybersecurity events. Solutions include Microsoft Defender for Endpoint Security, monthly CISA vulnerability testing, and 24/7 system activity and infrastructure performance monitoring and logging by AWS. Adjustments are made to processes and tools in response to preventable events, and remedial training is delivered to LinkIt employees as appropriate.
	<b>Detection Processes (DE.DP):</b> Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	LinkIt has established policies and procedures to identify and address anomalous events. These procedures are aided by third-party tools and service providers as noted above. LinkIt employees report suspicious events (e.g., phishing attacks or spoofed email identities from trusted LEA representatives) to the CISO for further action. Training based on specific experiences of such events is delivered to LinkIt team members.
<b>RESPOND (RS)</b>	<b>Response Planning (RS.RP):</b> 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. LinkIt has also implemented an Incident Response Plan and reporting documents based on NIST SP 800-61 and delivered training on that plan to all its team members. The company intends to facilitate a company-wide tabletop exercise (TTX) and perform a complete disaster response and recovery test in 1Q2025.
	<b>Communications (RS.CO):</b> Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	The LinkIt incident response plan (IRP) includes a section on communications with stakeholders, including applicable law enforcement. LinkIt records state and local privacy contacts (as defined in DPAs or other contracting vehicles) but has not yet recorded state and local law enforcement agencies. The IRP contains a matrix of internal roles and responsibilities to guide response activities.
	<b>Analysis (RS.AN):</b> Analysis is conducted to ensure effective response and support recovery activities.	LinkIt has established response and recovery procedures, inclusive of communication guidelines, that have been refined and improved over time. The company maintains a real-time status/availability page and can notify impacted clients at scale should such notification be appropriate. LinkIt also reviews how others in the K12 sector respond and communicate during recovery activities to improve its approach. Briefings from ISSA on how to control release of a security investigation "work product" have also informed LinkIt's communication strategy.



Function	Category	Contractor Response
	<b>Mitigation (RS.MI):</b> 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. Although specific actions may vary based on the severity and nature of the incident, the first actions taken after identification relate to its mitigation and can include protocols such as taking the database or web servers offline entirely pending further investigation and review. The IRP includes an event assessment rubric based on NIST SP 800-61.
	<b>Improvements (RS.IM):</b> 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 operational experience, internal testing, third-party review/recommendations, and incidents experienced by peer organizations. Such changes have been implemented to mitigate potential risks, rework processes, and address changes in the threat environment.
RECOVER (RC)	<b>Recovery Planning (RC.RP):</b> 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 to ensure restoration of data to a trusted state. The backup practices and tools used by its cloud service provider also promote confidence that restoration after an incident will be successful.
	<b>Improvements (RC.IM):</b> Recovery planning and processes are improved by incorporating lessons learned into future activities.	As with incident response practices, recovery practices are also informed by operational experience, including results of periodic testing to establish recovery benchmarks for systems with respect to business criticality, SLA timelines, recovery point objectives, etc. Although minimizing system downtime is a key priority, it is secondary to data confidentiality and integrity considerations.
	<b>Communications (RC.CO):</b> 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 activity planning includes coordination with internal and external parties under the direction of LinkIt's CTO and CISO. Although the specifics of the communications vary based upon incident circumstances and the target audience, keeping all stakeholders informed regarding the incident's status is a critical priority.