Acknowledgement of Third-Party Data Security Requirements

"District Data" refers to any information, data, records, files, or content, whether in digital or physical form, that is collected, processed, stored, generated or managed by the employees, students and contractors of the Hackensack Board of Education. This includes but is not limited to student records, educational materials, employee information, financial records, and any other data associated with the operations and activities of the Hackensack Board of Education. District Data encompasses both personal and non-personal information and is subject to the privacy and security provisions outlined in the District's Data Privacy and Security Policy (found at https://www.hackensackschools.org/privacy).

In addition to the terms specified in the District's Data Privacy and Security Policy, third party entities/individuals are expected to:

- Proactively identify and address information security risks that may impact the confidentiality, integrity and availability of the customer information it holds or processes as part of a documented information security/risk management process.
- Continually improve the company's ability to assess, detect, reduce, avoid and remediate information security risks and/or incidents.
- Work to avoid a negative impact to the District's reputation and brand as well as that of its stakeholders as a result of any security incident/breach.
- Comply with any applicable legal, regulatory or contractual requirements in respect to the confidential or protected data it holds about individuals (i.e., FERPA, COPPA, PPRA, HIPAA).
- Follow industry best practices for data collection, storage and security and secure coding (if applicable).
- Maintain a Data Security Policy outlining/governing, at a minimum:
    - Types of data collected along with rationale for collection
    - Data collection, storage and usage practices/procedures
    - Data security standards
    - Employee access to data
    - Disclosure/Sharing of District data with any other parties not directly contracted by the District/Customer
    - Policy review
    - Statement regarding how/when changes are made to the policy and how they will be communicated.
- Designate a Data Protection/Information Security Officer that, at a minimum, is tasked with:
    - Reviewing Data Protection/Security and related policies
    - Advising other staff on Data Security issues
    - Ensuring that Data Security induction and training takes place
    - Notification to stakeholders regarding data security-related developments
    - Handling subject access requests
    - Reviewing/Approving unusual or controversial disclosures of personal data
    - Reviewing/Approving contracts with Data Processors

HACKENSACK PUBLIC SCHOOLS

Acknowledgement of Third-Party Data Security Requirements

Below are a set of expected and required practices. Please indicate if you currently meet or do not meet each requirement/practice. Use the third column to provide any additional information you feel may elaborate your organization's specific practices. If a requirement or practice cannot be met as written, please provide an explanation as to what barriers prevent your organization from meeting the requirement and what compensating controls, if any, you may have in place.

Requirement/Practice	Yes	No	Compensating Control/Explanation
Encrypt District Data at-rest and in-transit using industry-standard encryption protocols such as AES-256 for data at-rest and TLS 1.2 or higher for data in-transit.	☐	☐	
Maintain access/change logs for a minimum of 90 days, conducting periodic reviews to identify and investigate any suspicious activity.	☐	☐	
Enforce multi-factor authentication for all employees and third parties accessing District Data or systems storing/handling District Data (excluding district users).	☐	☐	
Provide multi-factor authentication for district users with access to confidential/sensitive information, where applicable.	☐	☐	
Store all District Data in a facility compliant with ISO 27001 or NIST 800-53 standards, or an equivalent level of security, located in the United States or its territories.	☐	☐	
Conduct regular, automated backups of District Data daily, storing them securely offsite within the United States or its territories.	☐	☐	
Maintain and regularly test a documented data recovery plan to ensure timely restoration in case of data loss or system failures.	☐	☐	
Disclose to the District any agreements granting access to District Data between the vendor and third parties.	☐	☐	
Delete any data related to or created by a student upon request by a parent, verifying the request's validity by contacting the School or District.	☐	☐	
Establish and maintain comprehensive Disaster Recovery and Business Continuity Plans to ensure continuous services during fire, flash floods, pandemics, power outages, theft, and cyberattacks.	☐	☐	
Clearly outline responsibilities for all staff with access to District data during their induction procedures.	☐	☐	
Include Data Protection in foundational training for all staff.	☐	☐	

HACKENSACK PUBLIC SCHOOLS

Acknowledgement of Third-Party Data Security Requirements

Requirement/Practice	Yes	No	Compensating Control/Explanation
Ensure staff sign an electronic form indicating their understanding and acceptance of the organization's Data Security Policy.	☐	☐	
Classify data security incidents based on severity. a. Level 1: Classify unsuccessful exploit attempts as Level 1 - Non-Critical Incidents. b. Level 2: Classify incidents involving data loss as Level 2 - Critical Incidents, requiring notification to the District.	☐	☐	
Conduct annual reviews and audits of Data/Security Policies to ensure ongoing effectiveness and compliance.	☐	☐	
Perform annual penetration and vulnerability testing on all in-scope systems and networks. a. Address identified gaps within a reasonable timeframe, considering severity and exploitability of risks. b. Share non-specific/generalized information on identified gaps, including relevant vulnerability/risk scoring, and expected timeframes for resolution with the District within ten (10) business days.	☐	☐	

By signing below, I certify all information provided above is true and accurate to the best of my knowledge and that I am authorized to act on behalf of the business or organization submitting this document.

Name: _____

Title: _____

Company/Organization: _____

Signature: _____ Date: _____

Data Protection/Information Security Officer (if not the person completing this form):

Name: _____ Email: _____