

DATA PRIVACY AGREEMENT

Lancaster Central School District

This Data Privacy Agreement ("DPA") is by and between the **Lancaster Central School District** ("EA"), an Educational Agency, and Eyeread Inc. (aka Shoelace Learning)

("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 (EA):** 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 student 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 student 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 date services begin January 1, 2023 [date agreement is signed will populate upon signature]; Contractor may receive PII regulated by applicable 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 this DPA. 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.

5. 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 this DPA where the subcontractor will receive or have access to PII are consistent with those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. 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.
- (e) Contractor must not disclose PII to any unauthorized 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.

6. Training

To the extent required by law, the 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.

7. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its subcontractors retain PII or retain access to PII pursuant to the service agreement. Contractor will automatically delete all PII from its servers after a period of two (2) years following termination of the subscription, and from all backup servers after two (2) additional weeks. The EA may use the administrator portal to delete all PII at any time or may request assistance from Contractor to delete PII at any time. The confidentiality and data security

obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon deletion of PII from both active servers and backups.

8. Data Return and Destruction of Data

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, 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 prescribed by this agreement, or as expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. The EA may use the administrator portal to delete PII at any time or may request assistance from Contractor to do so. If not deleted by the EA, Contractor will automatically delete all PII from its servers after a period of no more than two (2) years following termination of the subscription, and from all backup servers after two (2) additional weeks.
- (b) 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) Upon request, 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.

9. Commercial or Marketing Use Prohibition

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose, except that teachers may receive email communications regarding product updates or professional development opportunities from which they may opt out at any time.

10. 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.

11. Breach

- (a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) calendar 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 mail, 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:

Michele Ziegler,
Data Protection Officer/Director of Instructional Technology and Accountability
Lancaster Central School District
177 Central Avenue
Lancaster, NY 14086
mziegler@lancasterschools.org

12. Cooperation with Investigations

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach of data governed by this DPA.

13. 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 actual 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.

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 this DPA, 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 this DPA, 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 this DPA 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.


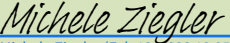
Contractor Name: Eyeread Inc. (aka Shoelace Learning)	
Signature:	 <small>Julia Rivard Dexter (Feb 10, 2023 13:40 MST)</small>
Printed Name:	Julia Rivard Dexter
Title:	CEO
Email:	julia@shoelacelearning.com
Date:	January 1, 2023
Lancaster Central School District Data Protection Officer – Michele Ziegler	
Date: Feb 13, 2023	Signature:  <small>Michele Ziegler (Feb 13, 2023 10:05 EST)</small>

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

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The Lancaster Central School District is committed to protecting the privacy and security of student protected data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

1. A student's personally identifiable information cannot be sold or released for any commercial purpose.
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 protected data elements collected by New York State (<http://www.nysed.gov/data-privacy-security/student-data-inventory>) is available for public review or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to submit complaints about possible breaches of student protected data or teacher or principal Annual Professional Performance Review data. Any such complaint must be submitted, in writing, to: Michele Ziegler, Director of Instructional Technology, 177 Central Avenue, Lancaster, New York 14086. Additionally, parents have the right to have complaints about possible breaches of student protected data addressed. Complaints should be directed to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234; the email address is "cpo@mail.nysed.gov". The State Education Department's complaint process is under development and will be established through regulations from the department's chief privacy officer, who has yet to be appointed.

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Lancaster Central School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

1. The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor;
2. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., Family Educational Rights and Privacy Act; Education Law Section 2-d);
3. The duration of the contract, including the contract’s expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
4. If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
5. Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to protect the data privacy and mitigate security risks; and
6. Address how the data will be protected using encryption while in motion and at rest.


Contractor Name: Eyeread Inc. (aka Shoelace Learning)	
Signature:	 <small>Julia Rivard Dexter (Feb 10, 2023 13:40 MST)</small>
Printed Name:	Julia Rivard Dexter
Title:	CEO
Email:	julia@shoelacelearning.com
Date:	January 1, 2023

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).

Description of the purpose(s) for which Contractor will receive/access PII	The exclusive purpose for which Vendor is receiving Protected Data from the District is to provide the district with functionality of the product or services listed above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within the Master Agreement.
Type of PII that Contractor will receive/access	Check applicable options: <input checked="" type="radio"/> Student PII <input type="radio"/> BOTH Student PII and APPR Data <input type="radio"/> APPR Data
Contract Term	Start Date: <u>January 1, 2023</u> End Date: Agreement remains in effect as long as the account is current and in good standing or upon expiration of the master agreement without renewal, or upon termination of the master agreement prior to its expiration.
Subcontractor Written Agreement Requirement	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="radio"/> Contractor will not utilize subcontractors. <input checked="" type="radio"/> Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: <input type="radio"/> Securely transfer PII to EA, or a successor contractor at the EA’s option and written discretion, in a format agreed to by the parties. <input checked="" type="radio"/> Securely delete and destroy PII.
Challenges to Data Accuracy	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 the Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA’s written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) <input checked="" type="radio"/> Using a cloud or infrastructure owned and hosted by a third party. <input type="radio"/> Using Contractor owned and hosted solution <input type="radio"/> Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:
Encryption	Data will be encrypted while in motion and at rest.

EXHIBIT B – Bill of Rights for Data Privacy and Security


Contractor Name: Eyeread Inc. (aka Shoelace Learning)	
Signature:	 <small>Julia Rivard Dexter (Feb 10, 2023 13:40 MST)</small>
Printed Name:	Julia Rivard Dexter
Title:	CEO
Email:	julia@shoelacelearning.com
Date:	January 1, 2023

EXHIBIT C - 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 review the following list and 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.**

CONTRACTORS ATTACHED PLAN SHALL INCLUDE THE FOLLOWING:

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.
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.
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.
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.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.
7	Describe your secure destruction practices and how certification will be provided to the EA.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 https://www.nist.gov/cyberframework/new-framework



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.

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	<ol style="list-style-type: none"> 1. Minimize data collection. Do not collect student data other than first name, initials, grade and parent email address and parent city and state. 2. Data at rest protected via multiple layers of operational security such as encryption, password protected access, need-to-know access. 3. Data in transit on school or public networks protected by industry-standard data encryption based on certificates and TLS security.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	<ol style="list-style-type: none"> 1. All access to production data tracked via work tickets 2. Only authorized users can view or download sensitive data 3. All employees and contractors are subject to a background check and must sign a contract and NDA with Shoelace Learning (Eyeread inc.)
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.	<ol style="list-style-type: none"> 1. Employees and contractors review documentation on our procedures and processes which is provided in our secure, protected, online library. 2. New employees and contractors are trained for 2 weeks on the standards and expectations, including policies and procedures.

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.	<ol style="list-style-type: none"> 1. All employees and contractors are subject to a background check and must sign a contract and NDA with Shoelace Learning (Eyeread inc.)
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.	<ol style="list-style-type: none"> 1. Breach or suspected breaches are detected by our monitoring and alerting systems and escalated according to rules to our theorized operators for further analysis. 2. If a breach of security or PII is detected, the incident management process begins. 3. Incident management process follows these stages: 4. a) gather information including the severity of the breach, 5. b) mitigate or stop the active breach by making technical changes 6. c) identify process or technical failures and preventative or remediating actions. 7. d) for high severity breaches, inform users of the data believed to have been leaked, our actions taken, and their suggested next steps (within 2 weeks),
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	<ol style="list-style-type: none"> 1. All “class” data may be downloaded or exported from the teacher dashboard at the conclusion of the school year, i.e. when the classes are closed either manually or automatically based on end date. 2. After a “class” has been closed in the teacher dashboard, then the data is no longer available for download. 3. Data for closed classes will be either deleted from our systems within 30 days, or anonymized and retained for research purposes for up to 20 years.

7	Describe your secure destruction practices and how certification will be provided to the EA.	<ol style="list-style-type: none"> 1. All digitally stored data is securely destroyed by deleting it from our databases and files. 2. We do not maintain physical equipment as everything is stored in a third party cloud. 3. We do not maintain physical copies of data.
8	Outline how your data security and privacy program/practices align with the EA’s applicable policies.	<ol style="list-style-type: none"> 1. We align with all applicable guidelines. 2. If there are any questions, please reach out to us at support@shoelacelearning.com for further clarifications.
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

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.	Aligned with ID.AM-2, ID.AM-6
	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.	Aligned with ID.BE-3, ID.BE-4.
	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.	We are familiar and aligned with our responsibilities and roles for cybersecurity.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Aligned with ID.RA-1
	Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Aligned with ID.RM-1
	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	We use tools to detect supply chain risks involving 3rd party libraries

Function	Category	Contractor Response
	established and implemented the processes to identify, assess and manage supply chain risks.	
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.	Aligned with PR.AC-1, PR.AC-4, PR.AC-7
	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.	We are aligned.
	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.	We are aligned
	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.	We are aligned
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	We are aligned with PR.MA-1, PR.MA-2
	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.	We are aligned with PR.PT-5.
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	We are aligned.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	We are aligned.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	The processes are informal today.
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	The processes are informal today.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	The processes are informal today.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	The processes are informal today.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	We are aligned.

Function	Category	Contractor Response
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	We are aligned.
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.	We are aligned.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	We are aligned.
	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).	We are aligned.