EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and "Contractor" is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Valley Stream UFSD 30 (the "District") and Contractor to the contrary, Contractor agrees as follows:

1. Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third-parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that the District's Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Children's Online Privacy Protection Act ("COPPA"), the Protection of Pupil Rights Amendment ("PPRA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any information rendered confidential by New York State ("State") or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by the District. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of the District as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of the District 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.

2. Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with District policy(ies) on data security and privacy. Contractor shall promptly reimburse the District for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of the District's data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Contractor's Data Security and Privacy Plan Requirements

3. Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of the District's Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

a. Outline how the Contractor will implement all State, federal, and local data security and privacy requirements over the life of the Agreement, consistent with the District's data security and privacy policy;
b. Specify the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
c. Demonstrate Contractor's compliance with the requirements of 8 NYCRR Part 121.3(c);
d. Specify how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and State laws governing confidentiality of such data prior to receiving access;
e. Specify how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
f. Specify how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the District;
g. Describe whether, how and when data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the Agreement is terminated or expires.

4. Pursuant to the Plan, Contractor will:

a. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5;
b. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;
c. Limit internal access to personally identifiable information to only those employees or subcontractors that need access to provide the contracted services;
d. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;
e. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

i. except for authorized representatives of Contractor such as a subcontractor or assignee to the extent they are carrying out the Agreement and in compliance with State and federal law, regulations and its Agreement with District; or
ii. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, District Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

f. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
g. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and
h. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

Contractor understands and agrees that it is responsible for submitting the above-referenced Data Security and Privacy Plan to the District prior to the start of the term of this Agreement. A copy of Contractor's Data Security and Privacy Plan is attached hereto as Exhibit "C". Further, Contractor shall sign a copy of the District's Parents Bill of Rights attached hereto as Exhibit "A".

Contractor's Supplemental Information Requirements

5. Contractor understands that, as part of the District's obligations under New York State Education Law § 2-d, Contractor is responsible for providing the District with supplemental information to be included in the District's Parents' Bill of Rights. Such supplemental information shall include:

a. The exclusive purposes for which the student data or teacher or principal data will be used;
b. How the Contractor will ensure that the subcontractors, persons or entities that the Contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
c. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the Agreement;
d. 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; and
e. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

The supplemental information required to be provided is included as Exhibit "B" and is incorporated by reference herein and made a part of this Agreement.

6. In the event of a breach of the within confidentiality and data security and privacy standards provision and unauthorized release of student data or teacher or principal data,

Contractor shall immediately notify the District and advise it as to the nature of the breach and steps Contractor has taken to minimize said breach. Said notification must be made in the most expedient way possible and without unreasonable delay but within no more than seven (7) calendar days of discovery of the breach. Notification required hereunder shall be made in writing and must, to the extent available, include a description of the breach, date of incident, date of discovery, the types of personally identifiable information affected, the number of records affected, a description of Contractor's investigation, and contact information for Contractor's representatives who can assist the District. Notification must be sent to the District's Superintendent of Schools with a copy to the District's Data Protection Officer. Notifications required under this paragraph must be provided to the District. at the following address:

Superintendent of Schools
Valley Stream UFSD 30
175 N. Central Avenue, Suite 220
Valley Stream, NY 11580

7. In the event that Contractor fails to notify the District of a breach in accordance with Education Law § 2-d, and/or Part 121 of the Regulations of the Commissioner of Education, said failure shall be punishable by a civil penalty of the greater of five thousand dollars ($5,000) or up to ten dollars ($10) per student, teacher and principal whose data was released, provided that the maximum penalty imposed shall not exceed the maximum penalty imposed under General Business Law § 899-aa(6)(a).

8. Except as provided in Education Law § 2-d(6)(d), in the event Contractor violates Education Law § 2-d, said violation shall be punishable by a civil penalty of up to one thousand dollars ($1,000). A second violation involving the same data shall be punishable by a civil penalty of up to five thousand dollars ($5,000). Any subsequent violation involving the same data shall be punishable by a civil penalty of up to ten thousand dollars ($10,000). Each violation shall be considered a separate violation for purposes of civil penalties and the total penalty shall not exceed the maximum penalty imposed under General Business Law § 899-aa(6)(a).

9. Contractor agrees that it will cooperate with the District 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 employees, agents, affiliates, or authorized users, as related to such investigations, will be the sole responsibility of the Contractor if such breach is attributable to the Contractor or its subcontractors.

10. Upon termination of this Agreement, Contractor shall return or, at the District's option, destroy all confidential information obtained in connection with the services provided herein and/or Protected Data. Destruction of the confidential information and/or Protected Data shall be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. Contractor further agrees that the terms and conditions set forth herein shall survive the expiration and/or termination of this Agreement.

11. In the event a Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the Contractor by State and federal law and Agreement shall apply to the subcontractor.

12. Where a parent or eligible student requests a service or product from Contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party Contractor for purposes of providing the requested product or service, such use by the third-party Contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor: EPS LEARNING

Signature: 

Date: December 12, 2025

Printed Name: Brent Goodman

Title: Bids & Contract Manager

EXHIBIT "A"

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Pursuant to New York State Education Law §2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information, as defined by Education Law §2-d. This document contains a plain-English summary of such rights.

- A student's personally identifiable information cannot be sold or released for any commercial purposes.
- Parents have the right to inspect and review the complete contents of their child's educational records maintained by the Valley Stream Union Free School District Thirty.
- State and Federal Laws protect the confidentiality of personally identifiable student information, and safeguards associated with industry standards and best practices, including, but not limited to, encryption, firewalls, and password protection must be in place when data is stored or transferred.
- A complete list of all student data elements collected by New York State is available for review at the following website: http://www.p12.nysed.gov/irs/sirs

The list may also be made available by writing to:

Office of Information & Reporting Services
New York State Education Department
Room 863 EBA,
89 Washington Avenue
Albany, NY 12234

Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Valley Stream UFSD 30
Attn: Data Protection Officer
175 N. Central Avenue, Suite 220
Valley Stream, New York 11580
Marcela Moran
516-434-3642

OR

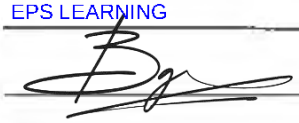
Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, NY 12234
Email: CPO@mail.nysed.gov

- Each contract with a third-party contractor which will receive student data, or teacher or principal data will include information addressing the following:
    - The exclusive purposes for which the student data or teacher or principal data will be used.
    - How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements.
    - When the agreement expires and what happens to the student data or teacher and principal data upon expiration of the agreement.
    - If and how a parent, student, a student over eighteen years of age, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and
    - Where the student data or teacher or principal data will be stored, and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

- Third-party contractors are also required to:
    - Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
    - Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
    - Not use educational records for any other purpose than those explicitly authorized in the contract;
    - Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
    - Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
    - Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
    - Notify the District of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
    - Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
    - Provide a signed copy of this Bill of Rights to the District thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

- This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

Contractor: EPS LEARNING

Signature: 

Date: December 12, 2025

Printed Name: Brent Goodman

Title: Bids & Contracts Manager

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).

Name of Contractor	**EPS Learning**
Description of the purpose(s) for which Contractor will receive/access PII	EPS Learning uses PII to deliver PreK–12 ELA, Literacy, Phonics, and math programs, provide customized professional development, support learning experiences, ensure secure product operation, improve products, offer customer support, enforce access controls, conduct system audits, and prevent fraud, as requested or authorized by the education agency and in compliance with applicable laws.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term	Contract Start Date _____ Contract End Date _____
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) ☐ Contractor will not utilize subcontractors. ☒ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • 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**.** • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If 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.
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)

	☒ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: *Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:* Protected Data is stored in secure U.S.-based data centers managed by EPS or controlled subcontractors. EPS Learning mitigates risks using a least-privileged access model, multi-factor authentication, Transport Layer Security for data in transit, and Advanced Encryption Standard (AES) for data at rest. Hosted on secure cloud infrastructure, data is protected by firewalls, password protection, and continuous monitoring, ensuring compliance with FERPA, COPPA, CIPA, and industry standards without compromising security.
Encryption	Data encryption is applied in accordance with Education Law 2-d. Data will be encrypted while in motion and at rest.
Training	Annual training on federal and state law governing confidentiality is provided for all officers, employees, or assignees who have access to student, teacher or principal data.

CONTRACTOR	**EPS Learning**
[Signature]	/S/ Brent Goodman
[Printed Name]	**Brent Goodman**
[Title]	**Bids & Contracts Manager**
Date:	**December 12, 2025**

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.*	EPS Learning operates on the principle that student data is the property of the Educational Agency (EA) and complies with the EA's guidance on data collection and storage. Systems and practices ensure appropriate handling and access to student data throughout the contract lifecycle, adhering to federal regulations such as FERPA, COPPA, and CIPA. Data is collected and used solely to support the learning experience, deliver EPS products, ensure secure and effective operation, improve products, provide customer support, or as otherwise requested/authorized by the EA.
2	*Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.*	**Administrative Safeguards**: Comprehensive data management procedures govern data collection, storage, access, retention, and disposal. Access is restricted using a least-privileged model, granting individuals only the rights necessary for their job functions. The EA retains ownership of all data. **Operational Safeguards**: A tiered support model routes client inquiries via an Issue Tracking System (JIRA) for efficient resolution. Customer Success Specialists conduct "Data Chats" to review student progress and provide data-driven guidance. **Technical Safeguards**: • **Encryption**: Data is encrypted in transit using protocols over TCP/IP and at rest using industry standard encryption algorithms. • **Secure Hosting**: Platforms are hosted on a secure cloud infrastructure, ensuring scalability and compliance with industry standards. • **Access Controls**: Multi-factor authentication for administrators, with encoded passwords. Access levels are defined for organizations, schools, tiers, districts, and system administrators. • **Monitoring and Auditing**: Telemetry and analytic data are collected for program improvement, with usage reports and logged user interactions.
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.*	Internal teams, including Sales Support, undergo rigorous training covering program facets, including compliance with federal and state data privacy laws (FERPA, COPPA, CIPA). Training equips employees to handle PII responsibly and is conducted internally for full-time employees, as extending it to external entities would be a significant burden.

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.*	EPS Learning signs Data Sharing Agreements (DSAs) with the EA to outline data handling terms, ensuring compliance with contractual obligations. Subcontractors, if utilized, operate under EPS Learning's direct control and are bound by the same security and privacy measures. The Sales Support team is trained to ensure consistent contract compliance.
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.*	EPS Learning communicates its data breach strategy within 5 days of becoming aware of a breach and will provide a summary of the written incident response plan containing non-proprietary information. The mitigation process includes isolating the breached component, determining scope and cause, restoring data and system operations, preventing future breaches, and analyzing the incident for lessons learned. An Incident Response Policy is available upon request and on receipt of a signed Non-Disclosure Agreement.
6	*Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.*	Upon contract expiration or termination, EPS Learning securely transfers data to the EA or a successor contractor, as directed in writing by the EA, in an agreed-upon format to ensure continuity and compliance with contractual obligations.
7	*Describe your secure destruction practices and how certification will be provided to the EA.*	Following data transition, EPS Learning performs Data Anonymization per industry standards and best practices, ensuring a robust data destruction process compliant with EA requirements, though specific certification is not detailed.
8	*Outline how your data security and privacy program/practices align with the EA's applicable policies.*	EPS Learning's program aligns with the EA's policies and complies with FERPA, COPPA, and CIPA. By recognizing student data as EA property and signing Data Sharing Agreements, EPS Learning ensures adherence to district-specific requirements. Industry best practices, including encryption, firewalls, and password protection, support alignment with the EA's security standards and the NIST Cybersecurity Framework.
9	*Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.*	**SEE EXHIBIT C.1 – NIST CSF TABLE ON THE NEXT PAGE**

BG

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
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.	**EPS Learning identifies and manages data, personnel, and systems, prioritizing student data as EA property. Data is handled per EA guidance and federal regulations (FERPA, COPPA, CIPA).**
	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.	**EPS Learning aligns its mission to support educational outcomes, prioritizing data privacy and defining roles for secure data management and customer support.**
	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.	**Policies and procedures ensure compliance with federal and state regulations. Data Sharing Agreements (DSAs) and internal processes guide regulatory and risk management.**
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**EPS Learning assesses risks to data and operations, implementing safeguards to protect PII and ensure system integrity.**
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**Risk tolerances are established, with practices like encryption and access controls to support operational risk decisions.**
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**Subcontractors, if used, operate under EPS's direct control, bound by DSAs and security measures to manage supply chain risks.**

Function	Category	Contractor Response
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.	**Access is restricted via a least-privileged model, with multi-factor authentication and SSHA-encoded passwords for authorized users.**
	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.	**Internal teams undergo rigorous training on data privacy laws (FERPA, COPPA, CIPA) and contract compliance.**
	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.	**Data is encrypted in transit (TLS 1.2+) and at rest (AES-256). Secure hosting on AWS ensures confidentiality and integrity.**
	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.	**Comprehensive policies govern data collection, storage, access, retention, and disposal, aligned with EA requirements.**
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**Systems are maintained via secure AWS infrastructure, ensuring operational continuity and compliance with security policies.**
	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.	**Technical solutions like encryption, firewalls, and usage monitoring ensure system resilience and security.**
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	**Telemetry and usage reports detect anomalous activity, with logged user interactions to assess event impact.**
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**Systems are monitored to identify cybersecurity events and verify the effectiveness of protective measures.**
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**Detection processes are maintained, with logged interactions and telemetry ensuring awareness of anomalies.**

Function	Category	Contractor Response
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**A defined process manages incidents, with a data breach strategy communicated within 5 days of detection.**
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**EPS Learning coordinates with the EA, providing an Incident Response Policy upon request to address incidents.**
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**Incident analysis determines scope, cause, and lessons learned to support recovery and prevent recurrence.**
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**Mitigation includes isolating breaches, restoring systems, and implementing measures to prevent future incidents.**
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**Lessons learned from incidents are incorporated to enhance response strategies and system security.**
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.	**Data and systems are restored post-incident, with secure data transfer to the EA or successor contractor upon contract end.**
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**Recovery processes are refined based on incident analysis to improve future resilience.**
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**Restoration activities are coordinated with the EA to ensure seamless data transition and system recovery.**