

EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

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

1. **Purpose**

- (a) This Exhibit supplements the Master License and Service Agreement (“MLSA”) to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as “Section 2-d”). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES’ Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES’ website.
- (b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service (“TOS”) that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

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

In addition, as used in this Exhibit:

- (a) “Student Data” means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.
- (b) “Teacher or Principal Data” means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.
- (c) “Protected Data” means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor’s Product.
- (d) “Participating Educational Agency” means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor’s Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another

BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

- (a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.
- (b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy. Erie 1 BOCES will provide Vendor with a copy of its policy. Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

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

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

- (a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.
- (b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA: **[Adhere to its published Privacy Policy (<https://www.imaginelearning.com/support/privacy/policy/>), including its Privacy Policy FAQ (<https://www.imaginelearning.com/support/privacy/privacy-faq/>)]**
- (c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.
- (d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.
- (e) Vendor **[check one]** _____ will ___x___ will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such

subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

- (f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.
- (g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

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

- (a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).
- (b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.
- (c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.
- (d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:
 - (i) the parent or eligible student has provided prior written consent; or
 - (ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.
- (e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;
- (f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.
- (g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

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

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

- (a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.
- (b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).
- (c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.
- (d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department (“CPO”). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.
- (e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

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

- (1) A student's personally identifiable information cannot be sold or released for any commercial purposes.
- (2) Parents have the right to inspect and review the complete contents of their child's education record.
- (3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
- (4) A complete list of all student data elements collected by the State is available for public review at <http://www.nysed.gov/data-privacy-security/student-data-inventory>, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
- (5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website <http://www.nysed.gov/data-privacy-security/report-improper-disclosure>.

BY THE VENDOR:

DocuSigned by:

David Alderslade

ED0E90F88BBB49B...

Signature

David Alderslade

Printed Name

CFO

Title

6/28/2023

Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT BETWEEN ERIE 1 BOCES AND IMAGINE LEARNING LLC

Erie 1 BOCES has entered into a Master License and Service Agreement (“MLSA”) with Imagine Learning LLC which governs the availability to Participating Educational Agencies of the following Product(s):

[Imagine Español, Imagine Language & Literacy, Imagine Math, Imagine Math Facts, MyPath, Pathblazer, and Social Emotional Learning (SEL) by Purpose Prep]

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

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

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements.

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on July 1, 2023 and expires on June 30, 2026.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.
- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has

disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

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

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

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

CONTRACTOR'S MODEL DATA PRIVACY AND SECURITY PLAN

Imagine Learning's Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations.

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Imagine Learning has designated a privacy official to manage the data security and privacy regulatory and contractual obligations involving personally identifiable information and student data.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect personally identifiable information (PII).	<p>In addition to the protections afforded by our cloud hosting providers, practices employed at Imagine Learning to protect personal data include, but are not limited to:</p> <p>Data encryption. Data is encrypted in transit and at rest.</p> <p>Access. Access to personal information is restricted to a limited number of Imagine Learning employees who need such access to perform their job.</p> <p>Data Systems Monitoring. Imagine Learning employs several third-party services that continuously monitor and scan our online services for vulnerabilities and misconfigurations. Employees dedicated to operating our services monitor these services and receive automated alerts when performance falls outside of prescribed norms.</p> <p>Incident Response Plan. Imagine Learning regularly reviews and maintains an incident response plan.</p> <p>File Transfer Protocol. Data is securely transferred to Imagine Learning using File Transfer Protocol (FTP) over secure (SSL/TLS) cryptographic protocol.</p> <p>Firewalls. Anti-virus software and firewalls are installed and configured to scan our systems. The firewall is periodically updated and configured so that users cannot disable the scans.</p> <p>Security audits. Imagine Learning conducts security audits and code reviews, both by outside providers and by executive summary.</p> <p>Secure programming practices. Imagine Learning software developers are aware of secure programming practices and strive to avoid introducing errors in our</p>

		<p>applications (such as those identified by OWASP and SANS) that could lead to security breaches.</p> <p>Account protection. Each user of Imagine Learning is required to create an account with a unique account name and password. Single Sign-On (SSO) users are authenticated with secure tokens.</p> <p>Facility security. Imagine Learning is located inside the continental United States. Physical access is protected by electronic access devices, with monitored security and fire/smoke alarm systems.</p> <p>Security Breach. In the event of a security breach that results in unauthorized release of personal data, Imagine Learning will notify affected customers of such breach, will investigate, and will restore the integrity of its data systems as soon as possible. We will fully cooperate and assist with required notices to those individuals affected by such breach.</p> <p>Employee Training. Imagine Learning has designated a privacy official to oversee employee security training and compliance.</p>
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.	All employees, agents and subcontractors are required to have at least annual privacy and data security training. Employees are also encouraged to received periodic role-based privacy training throughout the year.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	All employees are required to sign a confidentiality agreement that protects the confidentiality of customer information. Imagine Learning enters into written agreements with its service providers who will receive PII and student data where the service provider agrees to keep all data confidential and limit use of the data to those services for which they retained.
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 District.	In the event of a security or privacy incident that results in unauthorized release of personal data, Imagine Learning will notify affected customers of such breach in accordance with the terms of its contract with the customer, will investigate, and will restore the integrity of its data systems as soon as possible. We will fully cooperate and

		assist with required notices to those individuals affected by such breach.
6	Describe how data will be transitioned to the District when no longer needed by you to meet your contractual obligations, if applicable.	The data will be returned or deleted in compliance with the Data Privacy Agreement.
7	Describe your secure destruction practices and how certification will be provided to the District.	Imagine Learning destroys data in compliance with NIST SP 800-88 guidelines. Certification of destruction is provided to customer at the end of the services.
8	Outline how your data security and privacy program/practices align with the District's applicable policies.	Imagine Learning follows industry best practices, including the ISO 27001 Information Security Management Systems cybersecurity framework and NIST cybersecurity framework, throughout the development and maintenance lifecycle of our application.
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.

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.	Imagine Learning has policies and procedures for asset management including acceptable use, management and handling of assets.
	Business Environment (ID.BE): The organization's mission, objectives,	Imagine Learning has policies and procedures for organization of information security that includes

Function	Category	Contractor Response
	stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	security roles and responsibilities, contact with internal and external stakeholders, and project management of activities within the company.
	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.	Imagine Learning maintains ISO 27001 certification and employs security controls and policies to manage and monitor its cybersecurity risk in compliance with ISO 27001 standards.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Imagine Learning maintains policies and procedures for operations security to manage cybersecurity risks to operations, assets, and individuals.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Imagine Learning employs risk management strategies at the organization level such as third party audits, risk assessments, disaster recovery plan, and business continuity plan.
	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.	Imagine Learning has policies and procedures for supplier management including assessment of information security requirements of suppliers, address of security in supplier agreements and change management of supplier services.
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.	Imagine Learning has policies and procedure for access controls and physical and environmental security to limit access to systems, devices, processes and facilities.
	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.	Imagine Learning requires employees and partners to receive cybersecurity awareness education.
	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.	Imagine Learning maintains ISO 27001 certification and manages data in compliance with ISO 27001 requirements.

Function	Category	Contractor Response
	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.	Imagine Learning maintains privacy and security policies in compliance with ISO 27001 requirements to manage protection of information systems and assets.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Imagine Learning performs maintenance and repairs consistent with its 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 security solutions are assessed to ensure consistency with Imagine Learning security policies, procedures and agreements.
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	Imagine Learning monitors activities to detect vulnerabilities and any potential impact of those vulnerabilities.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Imagine Learning monitors information systems and assets to detect vulnerabilities and any potential impact of those vulnerabilities.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Detection processes are maintained and tested to ensure awareness of suspicious events.
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Imagine Learning has an incident response plan and playbook to respond to cybersecurity incidents.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Imagine Learning's incident response plan and playbook describe the appropriate communications with internal and external stakeholders.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Imagine Learning's incident response plan and playbook describe the process to analyze, investigate and respond to a cybersecurity incident.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Imagine Learning's incident response plan and playbook describe mitigation and remediation actions of a suspected or actual cybersecurity incident.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Imagine Learning's incident response plan and playbook describe postmortem activities to identify lessons learned and action items that need to be taken to improve services.

Function	Category	Contractor Response
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.	Imagine Learning maintains recovery policies and procedures to restore systems affected by cybersecurity incidents.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Imagine Learning's incident response plan describes postmortem activities to identify lessons learned and action items that need to be taken to improve services.
	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).	Imagine Learning's incident response plan and playbook describe the appropriate communications with internal and external stakeholders.

CONTRACTOR	
Signature	
Printed Name	
Title	
Date:	