

Exhibit A

DATA SHARING AND CONFIDENTIALITY AGREEMENT

Including

Clarence Central School District Bill of Rights for Data Security and Privacy
and
Supplemental Information about a Master Agreement between
Clarence Central School District and Screencastify, LLC

1. **Purpose**

(a) Clarence Central School District (hereinafter “District”) and Screencastify, LLC (hereinafter “Vendor”) are parties to a contract or other written agreement pursuant to which Vendor will receive student data and/or teacher or principal data that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as “Section 2-d”) from the District for purposes of providing certain products or services to the District (the “Master Agreement”).

(b) This Exhibit supplements the Master Agreement to which it is attached, to ensure that the Master Agreement conforms to the requirements of Section 2-d. This Exhibit consists of a Data Sharing and Confidentiality Agreement, a copy of the District’s Bill of Rights for Data Security and Privacy signed by Vendor, and the Supplemental Information about the Master Agreement between Clarence Central School District and Screencastify, LLC that the District is required by Section 2-d to post on its website.

(c) In consideration of the mutual promises set forth in the Master Agreement, Vendor agrees that it will comply with all terms set forth in the Master Agreement and this Exhibit. To the extent that any terms contained in the Master Agreement, or any terms contained in any other Exhibit(s) attached to and made a part of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In addition, in the event that Vendor has online or written Privacy Policies or Terms of Service (collectively, “TOS”) that would otherwise be applicable to its customers or users of the products or services that are the subject of the Master Agreement between the District and Vendor, to the extent that any terms of the TOS, that are or may be in effect at any time during the term of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

As used in this Exhibit:

(a) “Student Data” means personally identifiable information, as defined in Section 2-d, from student records that Vendor may receive from the District pursuant to the Master Agreement.

(b) “Teacher or Principal Data” means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Vendor may receive from the District pursuant to the Master Agreement.

(c) “Protected Data” means Student Data and/or Teacher or Principal Data, to the extent applicable to the product or service actually being provided to the District by Vendor pursuant to the Master Agreement.

(d) “NIST Cybersecurity Framework” means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the Master Agreement originates from the District and that this Protected Data belongs to and is owned by the District.

(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 the District’s policy on data security and privacy. The District will provide Vendor with a copy of its policy on data security and privacy upon request.

4. **Data Security and Privacy Plan**

As more fully described herein, throughout the term of the Master Agreement, Vendor will have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from the District.

Vendor’s Plan for protecting the District’s Protected Data includes, but is not limited to, its agreement to comply with the terms of the District’s Bill of Rights for Data Security and Privacy, a copy of which is set forth below and has been signed by the Vendor.

Additional components of Vendor’s Data Security and Privacy Plan for protection of the District’s Protected Data throughout the term of the Master Agreement are as follows:

(a) Vendor will implement all state, federal, and local data security and privacy requirements including those contained within the Master Agreement and this Data Sharing and Confidentiality Agreement, consistent with the District’s data security and privacy policy.

(b) Vendor will have specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the District under the Master Agreement.

(c) Vendor will comply with all obligations contained within the section set forth in this Exhibit below entitled “Supplemental Information about a Master Agreement between Clarence Central School District and Screencastify, LLC.” Vendor’s obligations described within this section include, but are not limited to:

- (i) its obligation to require subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) to execute written agreements acknowledging that the data protection obligations imposed on Vendor by state and federal law and the Master Agreement shall apply to the subcontractor, and
- (ii) its obligation to follow certain procedures for the return, transition, deletion and/or destruction of Protected Data upon termination, expiration or assignment (to the extent authorized) of the Master Agreement.

(d) Vendor has provided or will provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who will have access to Protected Data, prior to their receiving access.

(e) Vendor will manage data security and privacy incidents that implicate Protected Data and will develop and implement plans to identify breaches and unauthorized disclosures. Vendor will provide prompt notification to the District of any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement.

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

(a) Vendor will promptly notify the District of any breach or unauthorized release of Protected Data it has received from the District 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 the District by contacting the Clarence Central School District's Data Protection Officer directly by email at dpo@clarenceschools.org or by calling (716) 407-9100.

(c) Vendor will cooperate with the District and provide as much information as possible directly to Clarence Central School District's Data Protection Officer or his/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 Protected Data involved, an estimate of the number of records affected, the schools within the District 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, the District, 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 agrees not to provide this notification to the CPO directly unless requested by the District or otherwise required by law. 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 the District, Vendor will promptly inform Clarence Central School District's Data Protection Officer or his/her designee.

6. **Additional Statutory and Regulatory Obligations**¹

Vendor acknowledges that it has the following additional obligations under Section 2-d with respect to any Protected Data received from the District, and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach of the Master Agreement and the terms of this Data Sharing and Confidentiality Agreement:

(a) To limit internal access to Protected Data to only those employees or subcontractors that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA); *i.e.*, they need access in order to assist Vendor in fulfilling one or more of its obligations to the District under the Master Agreement.

¹ Nothing in Education Law Section 2-d or Part 121 specifically requires an educational agency to include within its contracts with third-party contractors this list of obligations that are imposed on third-party contractors by the statute and/or its implementing regulations. However, many school districts and other educational agencies have considered it a best practice to include these statutory and regulatory obligations within their third-party contracts.

(b) To not use Protected Data for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and the Master Agreement to which this Exhibit is attached.

(c) To not disclose any Protected Data to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations to the District and in compliance with state and federal law, regulations and the terms of the Master Agreement, 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 the District no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(d) To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.

(e) To use encryption technology to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

(f) To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

(g) To comply with the District's policy on data security and privacy, Section 2-d and Part 121.

(h) To not sell Protected Data 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.

(i) To notify the District, in accordance with the provisions of Section 5 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 applicable state or federal law, the District's Bill of Rights for Data Security and Privacy, the District's policies on data security and privacy, or other binding obligations relating to data privacy and security contained in the Master Agreement and this Exhibit.

(j) To cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

(k) To pay for or promptly reimburse the District for the full cost of notification, in the event the District is 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.

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The Clarence Central School District is committed to protecting the privacy and security of student 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 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 New York State is available for public review at the following website <http://www.nysed.gov/student-data-privacy/student-data-inventory> 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 have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, 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/student-data-privacy/form/report-improper-disclosure>.

APPENDIX

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 Clarence 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, as defined in the contract;
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., FERPA; 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 ensure the data will be protected and data privacy and security risks mitigated; and
6. Address how the data will be protected using encryption while in motion and at rest.

Screencastify, LLC

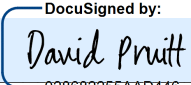
Company Name

David Pruitt

Printed Authorized Name

General Counsel

Title

DocuSigned by:

 028682255AAD446...

Authorized Signature

10/12/2023

Date

subject to attached addendum

**Supplemental Information about a Master Agreement between
Clarence Central School District and Screencastify, LLC²**

Clarence Central School District has entered into a Master Agreement with Screencastify, LLC, which governs the availability to the District of the following products or services:

See attached Addendum

Pursuant to the Master Agreement (which includes a Data Sharing and Confidentiality Agreement), the District may provide to Vendor, and Vendor will receive, personally identifiable information about students and/or teachers and principals that is protected by Section 2-d of the New York Education Law (“Protected Data”).

Exclusive Purposes for which Protected Data will be Used: The exclusive purpose for which Vendor is receiving Protected Data from the District is to provide the District with the functionality of the products or services listed above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within the Master Agreement.

Oversight of Subcontractors: In the event that Vendor engages subcontractors or other authorized persons or entities to perform one or more of its obligations under the Master Agreement (including subcontracting hosting of the Protected Data to a hosting service provider), it will require those subcontractors or other authorized persons or entities to whom it will disclose the Protected Data to execute legally binding agreements acknowledging their obligation under Section 2-d of the New York Education Law to comply with all applicable data protection, privacy and security requirements required of Vendor under the Master Agreement and applicable state and federal law and regulations.

Duration of Agreement and Protected Data Upon Termination or Expiration:

The Master Agreement commences on 8.1.23 and expires on 7.31.24.

- Upon expiration of the Master Agreement without renewal, or upon termination of the Master Agreement prior to its expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by the District, Vendor will assist the District in exporting all Protected Data previously received back to the District for its own use, prior to deletion, in such formats as may be requested by the District.

² Each educational agency, including a school district, is required to publish a “Bill of Rights for Data Security and Privacy” on its website. See, Education Law Section 2-d(3)(a) and Part 121.3(a). The Bill of Rights [that is posted on a district’s website] must also include “supplemental information” for each contract that the school district enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data [protected by Education Law Section 2-d]. See, Education Law Section 2-d(3)(c) and Part 121.3(c).

Nothing in Education Law Section 2-d or Part 121 requires an educational agency to post its third-party contracts on its website *in their entirety*. In addition, nothing in Education Law Section 2-d or Part 121 requires an educational agency to include the “supplemental information” about each contract, within the contract itself.

However, many school districts and other educational agencies have considered it a best practice to include most or all of the required elements of “supplemental information” within each applicable contract, and have complied with the obligation to include the “supplemental information” for each applicable contract with their Bill of Rights, by posting *the text from this page of this Exhibit* from each applicable contract (or a link to this text) on their website in proximity to their Bill of Rights.

- 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 the District 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 the District 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 the District to Vendor, by contacting the District regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may request to challenge the accuracy of APPR data provided to Vendor by following the appeal process in the District's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data that 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 (and, if applicable, its subcontractors) will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework, and safeguards associated with industry standards and best practices including, but not limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (and, 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 that complies with Section 2-d of the New York Education Law.



ADDENDUM TO DATA PRIVACY AGREEMENT

This Addendum supplements and modifies the Student Data Privacy Agreement (“**DPA**”) to which it is attached between Screencastify, LLC (“**Screencastify**”) and the applicable school district or local education agency (“**LEA**”) as such DPA applies to certain software and services Screencastify provides to LEA (the “**Services**”).

Screencastify and Customer agree to incorporate the following terms into the DPA:

1. **Provider MSA Terms.** Screencastify’s Services are subject to Screencastify’s Master Subscription Terms and Conditions located at www.screencastify.com/msa (“MSA Terms”) and such MSA terms are incorporated into the DPA, provided that if there is a direct conflict between the MSA Terms and the DPA, the DPA controls.
2. **Breach Notification.** The timeframe for any notification Screencastify is required to provide to LEA in connection with any unauthorized disclosure of personally identifiable information is within seven (7) days following Screencastify’s confirmation of such incident related to LEA’s personally identifiable information.
3. **Data Security and Privacy Plan.** To the extent the DPA requires Screencastify to submit supplemental information and/or a data security and privacy plan the attached Data Security and Privacy Plan is incorporated into the DPA.



**Ed Law 2d DATA SECURITY AND PRIVACY
PLAN**

Updated July 27, 2023

This Data Security and Privacy Plan (this "Plan") has been implemented and will be maintained by Screencastify, LLC ("Screencastify") in compliance with all applicable laws, including the New York Education Law §2-d ("§2-d") and regulations promulgated thereunder.

Screencastify will undertake industry standard practices, including physical controls, firewalls, and password protection, to protect the privacy and security of personally identifiable information ("PII") that Screencastify receives under each agreement (the "Agreement") with an educational agency customer subject to §2-d (the "Customer"), including alignment with the requirements of the National Institute for Standards and Technology ("NIST") Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

Screencastify will keep confidential all PII to which it has access in the performance of the Agreement. In addition to the above requirements, for PII:

1. **Purpose of Use.** Screencastify will use PII solely for the purpose of providing products and services to the Customer and as explicitly authorized in its agreement with Customer.
2. **Challenges to Accuracy / Deletion Requests.** As provided in Screencastify's Privacy Policy, if a parent or eligible student wishes to challenge the accuracy of or delete PII that is maintained by Screencastify, that request may be processed through the procedures provided by the Customer for amendment of education records under FERPA and the Customer may notify Screencastify of such request by emailing privacy@screencastify.com.
3. **Deletion of Customer Data.** Screencastify will delete Customer's PII so that it is physically and virtually irrecoverable within sixty (60) days of LEA's termination of its services relationship with Provider, and will provide the LEA with confirmation of such deletion upon written request.
4. **Subcontractor Oversight.** Screencastify's policy is to (i) vet prospective subcontractors and service providers who may handle PII on Screencastify's behalf to ensure they have acceptable controls in place to protect PII, (ii) only share PII with subcontractors, service providers and other third parties that are contractually bound to observe equally stringent obligations to maintain data privacy and security as are required of Screencastify pursuant to this Plan and (iii) regularly review its service providers with access to PII to ensure they continue to meet the requirements of this Plan.
5. **Security Practices and Procedures.** Screencastify has implemented the following security controls intended to provide reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the PII in its custody:
 - a. Screencastify has designated a privacy officer responsible for information security governance and maintains privacy policies and practices that support compliance with the Family Educational Rights and Privacy Act ("FERPA"), the Children's Online Privacy Protection Act ("COPPA") and other applicable laws.
 - b. PII is hosted in Google Cloud data centers located in the United States that maintain their own rigorous industry standard certifications and compliance offerings.



- c. Screencastify will comply with its privacy policy at <https://www.screencastify.com/privacy/policy>.
 - d. All provisions of the Customer's Parents' Bill of Rights for data privacy and security as required by New York Ed Law 2d are incorporated into this Plan.
 - e. Screencastify provides regular privacy and security awareness training, including training on applicable laws that govern the handling of PII, to its employees who will have access to PII.
 - f. Screencastify limits internal access to education records and PII to those individuals that are determined to have legitimate educational interests within the meaning of §2-d and FERPA; e.g., the individual needs access to the PII in order to fulfill his or her responsibilities in performing services to the Customer;
 - g. Screencastify uses encryption technology and other suitable means to protect the PII in Screencastify's custody, whether in motion or at rest, from unauthorized disclosure using a technology or methodology specified by the secretary of the U.S. Department of Health and Human Services in guidance issued under P.L. 111-5, Section 13402(H)(2), or any other technology or methodology specifically authorized by applicable statute, regulation or the New York State Education Department;
 - h. If Screencastify becomes aware of any breach of security resulting in an unauthorized release of Customer's PII by Screencastify or its subcontractors, Screencastify will notify Customer as required by applicable law or otherwise where Screencastify deems necessary to protect the safety and security of PII.
 - i. Screencastify uses a minimum encryption of AES256 for all data at rest and a minimum of TLS 1.3 for all data in transit.
6. **Further Amendments.** The parties acknowledge that an addendum to this Plan may be necessary to ensure compliance with §2-d following the promulgation of any additional regulations and/or the issuance of further guidance by the New York State Education Department subsequent to the execution of the Agreement. The parties agree to act in good faith to take such additional steps to amend this Plan as may be necessary at that time.
7. **NIST CSF Alignment.** The following chart demonstrates how Screencastify's information security program materially aligns with the NIST Cybersecurity Framework version 1.1.



EXHIBIT 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.	All devices, systems and facilities that enable the organization to achieve business purposes are carefully and diligently utilized and managed by board certified and licensed therapists who adhere to strict scopes of practice, ethical standards. Risk management team is put in place to assess and identify breach or security threat and will be handled in a systematic order to identify, assess, report and review any breach and to ensure there is no recurrence.
	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.	The mission, objectives, stakeholders and activities of the business are understood by all functioning members of the business and this information is regularly presented to each involved team member and reviewed in case of breach in order to review risk management decisions and processes
	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, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are presented frequently and inform the steps and process of handling and avoiding cybersecurity risks
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Yes, the organization understands all ramifications of cybersecurity risks and attacks. The organization has risk management assessment in place to ensure security. Risk responses are identified and prioritized
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	All organization risk management strategies are identified, established, assessed, managed and agreed to by all team members
	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.	All organization risk management strategies are identified, established, assessed, managed and agreed to by all team members
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.	Physical access to assets is managed and protected by authorized user.



	<p>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.</p>	Contractor's employees, officers, and/or subcontractors are trained and bound by the data protection and security requirements as a "Third-Party Contractor" as outlined in 8 NYCRR Part 121, in accordance with EA's Parents Bill of Rights and Supplemental Information to the Service Agreement
	<p>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.</p>	Data is protected when in use and not in use
	<p>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.</p>	Policies and regulations are in place regarding the use, management and oversight of information systems and assets
	<p>Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.</p>	Maintenance and repairs are performed in a secure way that prevents unauthorized access
	<p>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.</p>	Communications and control networks are protected
DETECT (DE)	<p>Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.</p>	Events are identified and assessed.
	<p>Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</p>	Vulnerability scans are performed.
	<p>Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.</p>	Detection processes are reviewed and modified for improvement
RESPOND (RS)	<p>Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.</p>	Response planning is executed during and after incident to avoid recurrence
	<p>Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).</p>	All team members understand roles when risk response is needed.



	<p>Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.</p>	All analysis is understood and processes are put in place to receive vulnerabilities and breach reports.
	<p>Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.</p>	Incidents will be contained, mitigated and kept on alert for risk
	<p>Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.</p>	Response strategies are continuously reviewed.
RECOVER (RC)	<p>Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.</p>	Recovery plan is performed during and after incident while strategies and procedures are continuously reviewed and updated.
	<p>Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.</p>	strategies and procedures are continuously reviewed and updated
	<p>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).</p>	Restoration activities include all parties involved in incident