EXHIBIT A: DATA SHARING AND CONFIDENTIALITY AGREEMENT

Including
Washington-Saratoga-Warren-Hamilton-Essex BOCES Bill of Rights for Data Security and Privacy
and
Supplemental Information about a Master Agreement between
Washington-Saratoga-Warren-Hamilton-Essex BOCES and Screencastify, LLC

1. Purpose

(a) **Washington-Saratoga-Warren-Hamilton-Essex BOCES, and on behalf of its subscribed school districts (see Exhibit B)** (hereinafter "District") and **Screencastify, LLC** (hereinafter "Vendor") are parties to a contract, Terms of Service, 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 **Washington-Saratoga-Warren-Hamilton-Essex BOCES and its subscribed school districts (see Exhibit B)** 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's policy on data security and privacy is available on the district website and at the following link: WSWHE BOCES Board of Education Policy #6810: Privacy & Security of Student Data, Teacher Data & Principal Data

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 **Washington-Saratoga-Warren-Hamilton-Essex BOCES** 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 **Cecilia Dansereau Rumley, Director for Data Privacy & Professional Learning** directly by email at **cdansereau-rumley@wswheboces.org** or by calling **518-581-3518.**

(c) Vendor will cooperate with the District and provide as much information as possible directly to **Cecilia Dansereau Rumley** 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 **Cecilia Dansereau Rumley** or his/her designee.

6. **Additional Statutory and Regulatory Obligations**

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.

(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.

Washington-Saratoga-Warren-Hamilton-Essex BOCES
EDUCATION LAW §2-d Bill of Rights for Data Security and Privacy

The **Washington-Saratoga-Warren-Hamilton-Essex BOCES** 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:

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and FERPA, includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including but not limited to encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available for public review at www.nysed.gov/data-privacy-security, and by writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of student data addressed.

   - Contact WSWHE BOCES Data Protection Officer: Cecilia Dansereau-Rumley, Director for Data Privacy & Professional Learning, by email: cdansereau-rumley@wswheboces.org, or by phone: 518-581-3518. Complaints should be submitted in writing using the form that is available on the BOCES website and in the BOCES offices.

   - Complaints may also be submitted to NYSED online at www.nysed.gov/data-privacy-security, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234, by email to privacy@nysed.gov, or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, the educational agency's policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

Subject to attached Addendum to Data Privacy Agreement, the terms of which are incorporated herein.

BY THE VENDOR: Screencastify, LLC

David Pruitt

Name (Print)

General Counsel

Title

DocuSigned by:
David Pruitt
028682255AAD446...

Signature

7/17/2023

Date

EXHIBIT A (CONTINUED)

Supplemental Information about a Master Agreement between

Washington-Saratoga-Warren-Hamilton-Essex BOCES and Screencastify, LLC

Washington-Saratoga-Warren-Hamilton-Essex BOCES and its subscribed school districts (see Exhibit B) has entered into a Master Agreement with **Screencastify, LLC,** which governs the availability to the District of the following products or services:

Screencastify
software, and/or apps, and/or technology tools, and/or web-services

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 **3/13/2023** and expires on **6/30/2026.**
- 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.

- 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.

Exhibit B:

School Districts Subscribed to the Washington-Saratoga-Warren-Hamilton-Essex BOCES Data Privacy & Security and/or Educational Technology and/or School Library Systems Cooperative Service Agreement(s)

Component School Districts	Other Subscribing School Districts
Argyle Central School	Beekmantown Central School District
Ballston Spa Central School	Broadalbin-Perth Central School District
Bolton Central School	Deposit Central School District
Cambridge Central School	Fonda-Fulton Central School District
Corinth Central School	Greater Amsterdam School District
Fort Ann Central School	Johnstown Central School District
Fort Edward Union Free School	Ravena Coeymans Central School District
Galway Central School	Rensselaer City School District
Glens Falls City School	Saranac Lake Central School District
Glens Falls Common District	Shenendehowa Central School District
Granville Central School	Walton Central School District
Greenwich Central School	Windsor Central School District
Hadley-Luzerne Central School	Willsboro Central School District
Hartford Central School	
Hudson Falls Central School	
Indian Lake Central School	
Johnsburg Central School	
Lake George Central School	
Mechanicville City School	
Minerva Central School	
Newcomb Central School	
North Warren Central School	
Queensbury Union Free School	
Salem Central School	
Saratoga Springs City Schools	
Schuylerville Central School	
South Glens Falls Central School	
Stillwater Central School	
Warrensburg Central School	
Waterford-Halfmoon Union Free School	
Whitehall Central School	

Screencastify

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 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 a data security and privacy plan the attached Data Security and Privacy Plan is incorporated into the DPA.

SCREENCASTIFY DATA PRIVACY AND SECURITY PLAN

This Data Privacy and Security Plan is prepared by Screencastify ("Contractor") and intended to serve as the Data Security and Privacy Plan required by Education Law § 2-d and Section 121.6 of the Commissioner's Regulations for the Educational Agency with whom Screencastify has contracted (EA) to provide software-as-a-service for video creation, editing and sharing.

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Contractor will implement applicable state, federal, and local data security and privacy contract requirements over the life of the Contract and only use PII in accordance with the Contract, and applicable laws pertaining to data privacy and security including Education Law § 2-d.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Contractor will maintain reasonable security standards appropriate to the type of data collected, which will include multiple safeguards to help protect against loss, misuse or alteration of information including encryption of data while in motion and at rest, regular software security updates and industry best practices for network and physical security.
3	Address the training received by your employees, officers and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII	Contractor will provide annual training to its officers, employees, or assignees who have access to PII on the federal and state law governing confidentiality of such data.
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.	Contractor will ensure that its employees, subcontractors and third-party service providers with whom Contractor shares PII abide by all applicable data protection and security requirements by entering into written agreements whereby such parties will perform

		their obligations in a manner consistent with the data protection and security requirements outlined therein.
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.	Contractor will promptly notify EA of any Breach or unauthorized release of PII in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such Breach that impacts EA PII. Contractor will cooperate with EA and law enforcement to protect the integrity of investigations into the Breach as provided in the DPA.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Contractor will delete EA's PII so that it is physically and virtually irrecoverable within sixty (60) days of EA's termination of its services relationship with Contractor, and will provide the EA with confirmation of such deletion upon written request. Through the services, EA will have the ability to recover and transfer any PII it wishes to maintain, and Contractor will cooperate with all efforts to do so.
7	Describe your secure destruction practices and how certification will be provided to the EA.	PII will be securely destroyed within 60 days of expiration or termination of the Contract using industry standard methods to ensure it is physically and virtually irrecoverable. Upon EA's request, Contractor will provide EA with certification of such destruction.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Contractor will implement the data protection and security requirements as a "Third-Party

		Contractor" as outlined in 8 NYCRR Part 121.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below. OR Outline how your data security and privacy program/practices materially align with the NIST CSF v 1.1. Please include details regarding how you will identify, protect, respond to, and recover from data security and privacy threats, as well as how you will manage your security controls.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – NIST CSF TABLE

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	All devices, systems and facilities that enable the organization to achieve business purposes are carefully and diligently utilized and managed. Information security 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

Function	Category	Contractor Response
	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 riskmanagement 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 information security committee 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 uses of business or its third party vendors.
	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	Contractor's employees who have a access to EA personal information are trained on privacy obligations and information security best practices on a regular basis.

Function	Category	Contractor Response
	consistent with related policies, procedures, and agreements.	
	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 classified according to risk level and is protected accordingly when at rest and in transit.
	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.	Policies and regulations are in place regarding the use, management and oversight 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.	Maintenance and repairs are performed in a secure way that prevents unauthorized access
	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.	Communications and control networks are protected
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Events are identified and assessed as part of Contractor's regular monitoring processes.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Vulnerability scans are performed on a regular basis.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Detection processes are reviewed and modified for improvement

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.	Response planning is executed during and after incident to avoid recurrence
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	All team members understand roles when risk response is needed.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	All analysis is understood and processes are put in place to receive vulnerabilities and breach reports.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Incidents will be contained, mitigated and kept on alert for risk
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Response strategies are continuously reviewed.
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.	Recovery plan is performed during and after incident while strategies and procedures are continuously reviewed and updated.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	strategies and procedures are continuously reviewed and updated
	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 include all parties involved in incident