

## **Appendix A**

### **Compliance With New York State Education Law Section 2-d Addendum (“Addendum”)**

The parties to this Agreement are the Monroe 1 Board of Cooperative Educational Services (“BOCES”) and [COMPANY], Inc. (“Vendor”). BOCES is an educational agency, as that term is used in Section 2-d of the New York State Education Law (“Section 2-d”) and its implementing regulations, and Vendor is a third party contractor, as that term is used in Section 2-d and its implementing regulations. BOCES and Vendor have entered into this Agreement to conform to the requirements of Section 2-d and its implementing regulations. To the extent that any term of any other agreement or document conflicts with the terms of this Agreement, the terms of this Agreement shall apply and be given effect.

#### Definitions

As used in this Agreement and related documents, the following terms shall have the following meanings: “Student Data” means personally identifiable information from student records that Vendor receives from an educational agency (including BOCES or a Participating School District) in connection with providing Services under this Agreement.

“Personally Identifiable Information” (“PII”) as applied to Student Data, means personally identifiable information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA), at 20 USC 1232g.

“Third Party Contractor,” “Contractor” or “Vendor” means any person or entity, other than an educational agency, that receives Student Data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including, but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs.

“BOCES” means Monroe #1 Board of Cooperative Educational Services.

“Parent” means a parent, legal guardian, or person in parental relation to a student.

“Student” means any person attending or seeking to enroll in an educational agency.

“Eligible Student” means a student eighteen years or older.

“State-protected Data” means Student Data, as applicable to Vendor’s product/service.

“Participating School District” means a public school district or board of cooperative educational services that obtains access to Vendor’s product/service through a cooperative educational services agreement (“CoSer”) with BOCES, or other entity that obtains access to Vendor’s product/service through an agreement with BOCES, and also includes BOCES when it uses the Vendor’s product/service to support its own educational programs or operations.

“Breach” means the unauthorized access, use, or disclosure of personally identifiable information.

“Commercial or marketing purpose” means the sale of PII; and the direct or indirect use or disclosure of State-protected Data to derive a profit, advertise, or develop, improve, or market products or services to students other than as may be expressly authorized by the parties in writing (the “Services”).

“Disclose”, “Disclosure,” and “Release” mean to intentionally or unintentionally permit access to State-protected Data; and to intentionally or unintentionally release, transfer, or otherwise communicate State-protected Data to someone not authorized by contract, consent, or law to receive that State-protected Data.

#### Vendor Obligations and Agreements

Vendor agrees that it shall comply with the following obligations with respect to any student data received in connection with providing Services under this Agreement and any failure to fulfill one of these statutory or regulatory obligations shall be a breach of this Agreement. Vendor shall:

(a) limit internal access to education records only to those employees and subcontractors that are determined to have legitimate educational interests in accessing the data within the meaning of Section 2-d, its implementing regulations and FERPA (e.g., the individual needs access in order to fulfill his/her responsibilities in providing the contracted services);

(b) only use personally identifiable information for the explicit purpose authorized by the Agreement, and must/will not use it for any purpose other than that explicitly authorized in the Agreement or by the parties in writing;

(c) not disclose any personally identifiable information received from BOCES or a Participating School District to any other party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Agreement, unless (i) if student PII, the Vendor or that other party has obtained the prior written consent of the parent or eligible student, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

(d) maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the personally identifiable information in its custody;

(e) use encryption technology to protect data while in motion or in its custody (i.e., in rest) from unauthorized disclosure by rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5 using a technology or methodology specified or permitted by the secretary of the U.S.);

(f) not sell personally identifiable information received from BOCES or a Participating School District nor use or disclose it for any marketing or commercial purpose unless otherwise expressly authorized by the Services, or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;

(g) notify the educational agency from which student data is received of any breach of security resulting in an unauthorized release of such data by Vendor or its assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay, in compliance with New York law and regulation;

(h) reasonably cooperate with educational agencies and law enforcement to protect the integrity of investigations into any breach or unauthorized release of personally identifiable information by Vendor;

(i) adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework, Version 1.1, that are in substantial compliance with the BOCES data security and privacy policy, and that comply with Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth below, as well as all applicable federal, state and local laws, rules and regulations;

(j) acknowledge and hereby agrees that the State-protected Data which Vendor receives or has access to pursuant to this Agreement may originate from several Participating School Districts located across New York State. Vendor acknowledges that the State-protected Data belongs to and is owned by the Participating School District or student from which it originates;

(k) acknowledge and hereby agrees that if Vendor has an online terms of service and/or Privacy Policy that may be applicable to its customers or users of its product/service, to the extent that any term of such online terms of service or Privacy Policy conflicts with applicable law or regulation, the terms of the applicable law or regulation shall apply;

(l) acknowledge and hereby agrees that Vendor shall promptly pay for or reimburse the educational agency for the full third party cost of a legally required breach notification to parents and eligible students due to the unauthorized release of student data caused by Vendor or its agent or assignee;

(m) ensure that employees, assignees and agents of Contractor who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access to such data; and

(n) ensure that any subcontractor that performs Contractor's obligations pursuant to the Agreement is legally bound by legally compliant data protection obligations imposed on the Contractor by law, the Agreement and this Agreement.

**Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security**  
(<https://www.monroe.edu/domain/1478>)

The Monroe #1 BOCES seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our operations.

The Monroe #1 BOCES seeks to ensure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the BOCES has posted this Parents' Bill of Rights for Data Privacy and Security.

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. The procedures for exercising this right can be found in Student Records Policy 6320. (<https://www.monroe.edu/6320>)
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 at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx> and a copy may be obtained 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:

Chief Privacy Officer  
New York State Education Department  
Room 863 EBA  
89 Washington Avenue  
Albany, New York 12234.

or  
Monroe One Data Protection Officer  
William Gregory  
Monroe #1 BOCES  
41 O'Connor Road  
Fairport, NY 14450

**Supplemental Information About Agreement Between [COMPANY] and BOCES**

(a) The exclusive purposes for which the personally identifiable information provided by BOCES or a Participating School District will be used by Vendor is to provide [COMPANY]'s [Student Safety services, including web filtering, classroom management, wellbeing analytics, and student threat detection] to BOCES or other Participating School District pursuant to a BOCES Purchase Order.

(b) Personally identifiable information received by Vendor, or by any assignee of Vendor, from BOCES or from a Participating School District shall not be sold or used for marketing purposes.

(c) Personally identifiable information received by Vendor, or by any assignee of Vendor shall not be shared with a sub-contractor except pursuant to a written contract that binds such a party to at least the same data protection and security requirements imposed on Vendor under this Agreement, as well as all applicable state and federal laws and regulations.

(d) The effective date of this Agreement shall be [4/11/2024] and the Agreement shall remain in effect until [6/30/2026], unless sooner by either party for any reason upon thirty (30) days' notice.

(e) Upon expiration or termination of the Agreement without a successor or renewal agreement in place, and upon request from BOCES or a Participating School District, Vendor shall transfer all educational agency data to the educational agency in a format agreed upon by the parties. Vendor shall thereafter securely delete all educational agency data remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies) as well as any and all educational agency data maintained on behalf of Vendor in secure data center facilities, other than any data that Vendor is required to maintain pursuant to law, regulation or audit requirements. Vendor shall ensure that no copy, summary or extract of the educational agency data or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the secure data center facilities unless Vendor is required to keep such data for legal, regulator, or audit purposes, in which case the data will be retained in compliance with the terms of this Agreement. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers permanently removed with no possibility of reidentification), they each agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to the BOCES or Participating School District from an appropriate officer that the requirements of this paragraph have been satisfied in full.

(f) State and federal laws require educational agencies to establish processes for a parent or eligible student to challenge the accuracy of their student data. Third party contractors must cooperate with educational agencies in complying with the law. If a parent or eligible student submits a challenge to the accuracy of student data to the student's district of enrollment and the challenge is upheld, Vendor will cooperate with the educational agency to amend such data.

(g) Vendor shall store and maintain PII in electronic format on systems maintained by Vendor in a secure data center facility in the United States in accordance with its Privacy Policy, NIST Cybersecurity Framework, Version 1.1, and the BOCES data security and privacy policy, Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education, and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth above. Encryption technology will be utilized while data is in motion and at rest, as detailed above.

(h) A copy of Vendor's Data Privacy and Security Plan, which vendor affirms complies with 8 N.Y.C.R.R. 121.6 is attached hereto as **Attachment 1** and is incorporated herein by reference as if fully set forth herein.

DocuSigned by:  
Harrison Parker

Jun 4, 2024 | 11:53 AM PDT

Vendor Signature



# ATTACHMENT 1 - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

## CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	We operate under a NIST-CSF framework and have an established set of policies, processes and procedures as described below. Requirements will be specified via Service Level Agreements and/or Data Processing Agreements.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	<p><b>Administrative Safeguards:</b></p> <p>Established set of Privacy Policies and Procedures: These documents outline how PII is collected, used, stored, and shared.</p> <p>Access Controls to limit access to PII based on job roles and responsibilities. Implement role-based access controls (RBAC) to ensure only authorized personnel can access sensitive data.</p> <p>Training and Awareness on privacy practices, security protocols, and their responsibilities regarding PII protection.</p> <p>Incident Response, Data Breach Plans and Risk Assessments to identify vulnerabilities and prioritize security measures.</p> <p><b>Operational Safeguards:</b></p> <p>Backup and Recovery: Regularly back up PII and test data restoration processes.</p>

		<p><b>Audit Trails:</b> Maintain logs of system activities to track access, changes, and incidents related to PII.</p> <p><b>Secure Disposal:</b> Properly dispose of PII (e.g., shredding paper documents, wiping hard drives) to prevent unauthorized retrieval.</p> <p><b>Third-Party Risk Management:</b> Assess and monitor security practices of vendors and partners who handle PII.</p> <p><b>Technical Safeguards:</b></p> <p><b>Encryption:</b> Encrypt PII during transmission (e.g., TLS) and storage (e.g., data-at-rest encryption).</p> <p><b>Intrusion Detection Systems (IDS):</b> We deploy a number systems (CrowdStrike, JupiterOne, Splunk, DataDog, Sentra) to detect and respond to suspicious activities.</p> <p><b>Access Authentication:</b> Implement strong authentication mechanisms (e.g., multi-factor authentication and SSO) to verify user identities.</p> <p><b>Data Masking and Redaction:</b> Hide sensitive PII within databases or documents to limit exposure and track through use of a data discovery utility (Sentra).</p> <p><b>Regular Security Updates:</b> Keep software, operating systems, and applications up-to-date to address known vulnerabilities.</p>
3	<p>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.</p>	<p>We confirm that we comply with the applicable state law and regulations. We will train all employees with access to your data on the requirements of state and federal law governing the confidentiality of such data. We will require all subcontractors to comply with the terms of this Privacy Policy, including its terms on data breach.</p>

		<p>As a provider of cyber safety products to schools in the United States we act as a school official, operating under your direction and control. In this capacity, we have a legitimate educational interest in the collection, use, disclosure, and retention of information with respect to your students and staff.</p> <p>We are committed to complying with the Family Education Rights and Privacy Act ("FERPA"), the Children's Online Privacy Protection Act ("COPPA")</p>
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.	Employees are bound by clauses within their contract of employment which specifically involves regulation of personal information. Data Processing Agreements and SLA's are used for sub-contractors and vendors.
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.	Qoria has a mature and tested data breach policy which clearly identifies roles and responsibilities, forensic investigation process, communicating out to stakeholders and other interested parties such as the regulator.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Under the terms and conditions of the contract, we would expect this to be specified as per SLA or DPA. As the data processor, we will always carry out the instructions of the data controller within reason.
7	Describe your secure destruction practices and how certification will be provided to the EA.	We use third party vendors for the destruction of confidential waste and equipment. Destruction certificates are received by Qoria from the vendor upon destruction. For destruction of



		customer data by Qoria, we can provide destruction certificates on request.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	We will adhere where practically possible with EA's applicable policies.
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.

### ATTACHMENT 1(A) – 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)	<b>Asset Management (ID.AM):</b> 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.	Coverage of devices and platforms are cataloged and inventoried using CrowdStrike and JupiterOne to automate system inventory and asset management which enables tracking, updating, prioritizing, monitoring and reporting of the asset inventory inclusive of a detailed data classification scheme. Cybersecurity roles and responsibilities are also established within the organization and an asset management process/policy is established.
	<b>Business Environment (ID.BE):</b> 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.	Mission and objectives clearly defined by the board and directors with business risks and opportunities are identified through business impact analyses and laid down in the risk register. Business resilience is maintained through policies and procedures as well as Incident Response Management, Business Continuity and Disaster recovery plans and procedures.
	<b>Governance (ID.GV):</b> The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	We have an established set of security & privacy policies that forms the overarching ISMS. This includes acceptable use, third party risk management, internal privacy policy, end user account security policy, user device security policy, data classification policy, data breach policy, admin and resource account security policy, security vulnerability management policy and more. Our staff are trained on these annually as part of cyber awareness training, and we also require staff to sign out internal privacy policy as well as our acceptable use policy. Risks are logged and controlled in our risk register and undergo risk treatment as part of our risk management methodology.

Function	Category	Contractor Response
	<p><b>Risk Assessment (ID.RA):</b> The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.</p>	<p>As well as the group risk register encompassing tech risks and business risks, as part of the NIST CSF framework, products/departments undergo an organizational level risk analysis based on NIST 800 control set to identify threat/vulnerability/risk as well as vulnerabilities to attack vectors. Risk treatment plan is established for key risks and vulnerabilities</p>
	<p><b>Risk Management Strategy (ID.RM):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</p>	<p>A comprehensive, industry standard risk management framework is in place which evaluates potential impacts, both business and technical by identifying the severity of threat and subsequent control effectiveness. Risk appetites are formally defined and communicated with risk tolerance and treatment levels determined.</p>
	<p><b>Supply Chain Risk Management (ID.SC):</b> 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.</p>	<p>A mature and tested third party risk management process is in place to ensure vendors meet security, privacy and regulatory requirements before use by Qoria. Process requires sign-off from management prior to onboarding of third party vendors. Monitoring continues through regular reviews to ensure business continuity and relevant accreditations are still in place. Vendors not meeting criteria are not used.</p>
PROTECT (PR)	<p><b>Identity Management, Authentication and Access Control (PR.AC):</b> 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.</p>	<p>Access control and acceptable use policies in place. Endpoint devices are controlled through JupiterOne and CrowdStrike. Onboarding and Offboarding policy and process dictates principles of least privilege and separation of duties. MFA and SSO are used as part of access control and password protection enforced through password management utility.</p>
	<p><b>Awareness and Training (PR.AT):</b> 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>	<p>Formal infosec/privacy training is given within the first two weeks of starting with the company and subsequent annual refresher training is carried out. InfoSec knowledge repository is held on company intranet and Security/Privacy updates are communicated through the company chat channels. Specialized training is given to those in security related roles and all individuals within the company are made aware of their roles and responsibilities when accessing information and systems. Processes, policies and procedures are defined and made available to all staff.</p>
	<p><b>Data Security (PR.DS):</b> Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.</p>	<p>Baseline encryption controls are in place for data in transit and at rest, encryption keys are managed and all data is monitored through the use of a data discovery tool which monitors data movement. Assets are managed and monitored through CrowdStrike and JupiterOne to ensure checking mechanisms are in place to detect unauthorized installation of software, changes to applications and information. Development and testing environments are separated and monitored through data discovery tool (Sentra).</p>

Function	Category	Contractor Response
	<b>Information Protection Processes and Procedures (PR.IP):</b> 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.	Overarching set of policies (see ID.GV) in place to form ISMS, vulnerability management process in place, onboarding and offboarding and change management policies. Endpoints protected by JupiterOne and Crowdstrike. Incident response plan in place which is tested periodically internally and via external partner. Pen tests carried out at least annually with remediation plans in place for rectification. System Development Life-Cycle process in place which requires specific attention to security and privacy with sign-off required by both privacy and security before approval. Backups are carried out, maintained and tested.
	<b>Maintenance (PR.MA):</b> Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Maintenance and support schedules are kept though much of our infrastructure is kept within the cloud through GCP, AWS, Azure and VM's
	<b>Protective Technology (PR.PT):</b> Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Full suite of policies and procedures in place to form the overarching ISMS. Audits and logging is carried out as well as a vulnerability management process and annual penetration testing.
<b>DETECT (DE)</b>	<b>Anomalies and Events (DE.AE):</b> Anomalous activity is detected and the potential impact of events is understood.	Security Operations Center (SOC) is used to provide 24/7 network monitoring and alerts and detected events are analyzed through impact analysis/lessons learned.
	<b>Security Continuous Monitoring (DE.CM):</b> The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Monitoring of the network through the SOC and monitoring of asset and endpoints through Crowdstrike and JupiterOne
	<b>Detection Processes (DE.DP):</b> Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Monitoring and detection through SOC, Crowdstrike and JupiterOne. Processes are regularly tested and communicated across to interested parties and incident management includes lessons learned/improvement.
<b>RESPOND (RS)</b>	<b>Response Planning (RS.RP):</b> Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Incident Response Plan is in place and is audited/tested through external audit scenario playthroughs..
	<b>Communications (RS.CO):</b> Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Roles and responsibilities are defined within the Incident Response Plan as are internal and external stakeholders. Playbooks are maintained and shared with stakeholders.
	<b>Analysis (RS.AN):</b> Analysis is conducted to ensure effective response and support recovery activities.	Investigations and impact analysis are carried out, all alerts and notifications are investigated by the security team and understood through forensic analysis and vulnerability management process.
	<b>Mitigation (RS.MI):</b> Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Incident Response and disaster recovery plans involve containment and mitigation stages with developed strategies established for multiple incident types. Newly identified vulnerabilities are documented in the risk register and undergo the risk management process.
	<b>Improvements (RS.IM):</b> Organizational response activities are improved by incorporating lessons learned from	Incident response plan involves a 'lessons learned' stage which involves after-action reports, vulnerability and risk management and is documented in the knowledge base.

Function	Category	Contractor Response
	current and previous detection/response activities.	
RECOVER (RC)	<b>Recovery Planning (RC.RP):</b> Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Formal Incident Response Plan and Business Continuity/Disaster Recovery plan is in place. Plans are tested through both internal and external audit and through play-through scenarios.
	<b>Improvements (RC.IM):</b> Recovery planning and processes are improved by incorporating lessons learned into future activities.	Our internal and external audits, testing and scenario playthroughs are key elements of the continuous improvement process.
	<b>Communications (RC.CO):</b> 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).	Covered within the Disaster Recovery/Business Continuity plan is the communication out to all stakeholders, the management of public relations, managing of reputational effects, repair and recovery which is communicated to all involved.