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.	ImPACT Applications has implemented many policies and procedures as it relates to the security, privacy and availability of our application environments. We undergo annual SOC 2 Type II audits by an independent third-party auditor covering the domains of security, privacy and availability. ImPACT Applications has also achieved ISO 13485 certification for our quality management system. We've also ensured HIPAA Privacy and Security rule compliance.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Administrative, physical and technical safeguards, in congruence with HIPAA's privacy and security rules are part of our company's quality management system and are ingrained in the normal business operations practices. Risk analysis, access control and authorization, physical facility access policies, data backup and encryption all are part of policies that are in place.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Employees receive training on data privacy and security, HIPAA compliance, various cybersecurity topics and many other internal training courses that are relevant to the employee's job position. These training courses are assigned by the Director of Regulatory Affairs and are tracked through an online system to ensure employee compliance.

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 required to read and acknowledge our employee handbook, as well as several other employment related documents upon the start of their employment with the company. Employment doesn't start until all of these agreements are signed.
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.	Any data security and privacy incidents will undergo discovery and risk assessment, identification of the cause and extent of the breach, foreseeable harm of the breach, and notification of affected customers. Notification to affected customers will occur within 48 hours of becoming aware of the breach.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Customers are able to export their data at any time via the ImPACT Applications Customer Center.
7	Describe your secure destruction practices and how certification will be provided to the EA.	When a machine or hard drive is decommissioned and has been used by an employee with access to Personal Information, the drive must be securely erased or destroyed before the machine, or its hard drive can be relinquished from the company's control. DBAN is our utility of choice, a disk image for a bootable CD can be found at https://dban.org. If the drive has failed, and will not complete a DBAN destruction attempt, the drive must be physically destroyed so the platters inside are crushed, and it is not usable any longer. Document template QT-18 is to be used to create a record of the data destruction, signed, and stored as evidence of the completed action. Data deleted from our production databases as part of our data deletion processes is identified and removed based on the age of the records, and the data retention settings of the

		customer organization. Data is removed by an automated process, executing sql statements to remove the specified information from our online databases. The number of records before and after a data deletion event can be provided to confirm the removal of data.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Our data security practices were designed to meet and exceed the requirements set by HIPAA and many other state/local entities. Our policies and procedures have been audited as part of our ISO 13485 certification and SOC 2 Type 2 annual audits.
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)	**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.	Our systems are housed in a secure datacenter facility, within a locked cabinet. Only authorized employees have access to the computing environment. Access to environments (physical or logical) must be approved by management and allocated to each individual user. Hardware assets are tracked by serial number. The company follows a joiners & leavers process to ensure accounts are provisioned and deprovisioned in a timely fashion. We employ VPNs and MFA to provide secure access for our employees.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this	Our employee handbook defines expected employee behavior. Job descriptions outline roles and responsibilities. Our quality management system helps to assess and manage risk, ensuring our products are secure and compliant from design to delivery.

Function	Category	Contractor Response
	information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Our ISO 13485 certification and annual SOC 2 Type 2 audits are instrumental in helping to ensure these policies are followed.
	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.	Our ISO 13485 quality management system has policies and procedures for managing and monitoring the organization's regulatory, legal, risk, and operational requirements. The policy is distributed to applicable employees, and those that have participatory roles are trained on their responsibilities regarding these policies.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ImPACT Applications has controls, procedures and policies in place to reduce and mitigate as much as possible any cybersecurity risk to organizational operations, data, assets, and individuals, including but not limited to secure development practices, network and internet boundary protections, and server protections.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ImPACT Applications has a comprehensive risk management strategy that is part of our overall quality management system.
	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.	ImPACT Applications has implemented a vendor evaluation and purchasing process to vet vendors and their products prior to purchase, ensuring they meet the designated criteria for their function.
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.	ImPACT Applications follows a Joiners and Leavers process that requires approval for account creation and prompt termination of access that is no longer necessary. This process is audited as part of our annual SOC 2 Type 2 audit.
	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.	ImPACT Applications has an employee training program in place and routinely assigns training exercises to employees on an as-needed basis. All employees receive a base-level of training when their employment begins, and additional items are added depending on job function and industry changes.
	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.	ImPACT Applications ensures all sensitive PII and PHI data are handled appropriately, stored in secure locations, and encrypted in transit and while at rest in our application database.

Function	Category	Contractor Response
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	ImPACT Applications has a comprehensive set of IT policies and procedures, reviewed and approved by management that are followed and audited as part of our annual SOC 2 Type 2 audit.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	ImPACT Applications' IT policies and procedures contain sections addressing maintenance and patching of our systems.
	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.	ImPACT Applications periodically reviews all firewall rules associated with our application environments to ensure they are appropriate for our application needs. Any changes to the firewall rule set need to be reviewed and approved by management prior to being implemented.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	All servers run HIDS software to monitor for any intrusion attempts and are configured to notify ImPACT Applications system administrators immediately if any anomalies are detected.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	ImPACT Applications monitors all servers with standard server & resource monitoring software to ensure they are operating properly. Additionally, we perform quarterly vulnerability scans and annual application security scans to check for and resolve any vulnerabilities found.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	HIDS and WAF configurations are reviewed periodically to ensure proper configuration and notification is in place.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	ImPACT Applications has a series of policies and procedures in place in the event a security event occurs. This policy includes information about notification requirements and time periods, investigation, and remediation.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	ImPACT Applications has a defined breach notification procedure that defines the tasks to complete, who to involve, when notifications are to go out and what they should contain.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	ImPACT Applications procedures include analysis phases to ensure an incident is sufficiently investigated to ensure the root problem is identified and corrected.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	ImPACT Applications will work to contain and limit the impact of any security event as quickly as possible, while preserving any information that would be helpful in investigating the root cause of the incident.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	ImPACT Applications will take appropriate actions to mitigate or correct any issues that resulted in the origination of the incident to prevent any reoccurrence in the future.

Function	Category	Contractor Response
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	ImPACT Applications has a disaster recovery policy in place, tests the procedure annually, and ensures any required changes to the policy are made as needed.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	As part of our disaster recovery testing process, any lessons learned are incorporated into the policy so that it is continuously improved and accurate for current systems/applications.
	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).	ImPACT Applications has direct lines of communication with critical service providers, monitors communications and status pages for providers, alert messages and notifications from critical vendors. We subscribe to notification lists for services, software vendors and other service providers so that we can be aware of any service interruptions that may affect our services and customers.