## 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. | Yearly cyber security and student safety/data training Additional training as necessary. |
| 2 | Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII. | Follow all local, state and federal guidelines. Collect minimal PII Quarterly audits. Platform student data disposed each summer. |
| 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. | Yearly cyber security and student safety/data training Additional training as necessary. |
| 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. | Yearly cyber security and student safety/data training Additional training as necessary. |
| 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. | See attached document for plan. |
| 6 | Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable. | When requested, data will be transitioned to district up to industry standards. |

| | | |
|---|---|---|
| 7 | Describe your secure destruction practices and how certification will be provided to the EA. | Destruction practices are up to industry standards and completed each summer. Certification available upon request. |
| 8 | Outline how your data security and privacy program/practices align with the EA's applicable policies. | See attached document for plan. |
| 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. |

## EXHIBIT C.1 – 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

| 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 NLP Assets are assigned to individual employees and tracked for the purposes of day-to-day business and risk mitigation. These assets (including physical and data) are reviewed annually or as needed (such as when an employee leaves the organization.) |
| | **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. | NLP believes in ensuring and implementing industry standards and best practices to keep internal data secure and protect the data of our clients. These standards and practices drive decision making, selection of employees and day to day implementation of NLP mission and vision. |
| | **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. | The Senior NLP Leadership Team (including the CEO and all Senior VPs) are tasked with ensuring the business environment is sustained in such a way that protects all NLP interests and the interests of our clients. Policies and practices are review annual (or as needed) to ensure they meet industry standards and best practices. |
| | **Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. | NLP retains the services of experienced attorney's to review all risk to the organization as well as any risk to NLP clients. These reviews occur annually and information gathered is used to drive changes and updates to policy or creation of new polices as needed. |

| Function | Category | Contractor Response |
|---|---|---|
| | **Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. | Clients trust NLP with their data and therefore we understand the need to mitigate risk. The NLP Senior Leadership Team is tasked with examining current practices and, with the advice of the Risk Management Evaluation make any necessary changes to mitigate any risks discovered. |
| | **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. | Not applicable |
| **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. | All users are required to use NLP provided logins and 2FA in order to gain access to NLP systems.<br><br>Only those users with a legitimate business purpose are able to access sensitive systems where client data is housed. All data centers are under the control of a third party and access to these physical locations is tightly controlled. |
| | **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. | Yearly cyber security and student data privacy training for all members of The News Literacy Project and subcontractor. |
| | **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. | Only users with a legitimate business purpose may access any data or systems that house or contain customer PII. |
| | **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. | All users are required to use NLP provided logins and 2FA in order to gain access to NLP systems.<br><br>Only those users with a legitimate business purpose are able to access sensitive systems where client data is housed. All data centers are under the control of a third party and access to these physical locations is tightly controlled. |
| | **Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures. | NLP and its subcontractor follow industry standards and best practices on maintenance. All updates to the platform are first tested in a Pre-Production Environment and QA conducted before releasing to Production. All Production environments are monitored for any impacts to clients post maintenance and at all times. |
| | **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. | NLP and its subcontractor utilize Amazon Web Services (AWS) for hosting and monitoring of the platform. They maintain a SOC II for all hosting environments. The NLP subcontractor also used industry standard monitoring solutions to ensure platform stability and security. |

| Function | Category | Contractor Response |
|---|---|---|
| DETECT (DE) | **Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood. | The NLP subcontractor uses industry standard monitoring solutions to ensure platform stability and security. If an event is detected its potential impact is reviewed immediately and any required mitigation procedures performed. |
| | **Security Continuous Monitoring (DE.CM):** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. | The NLP subcontractor uses industry standard monitoring solutions to ensure platform stability and security. If an event is detected its potential impact is reviewed immediately and any required mitigation procedures performed. |
| | **Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. | These detection systems are reviewed by the subcontractor for effectiveness as needed. |
| RESPOND (RS) | **Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents. | NLP maintains rigorous response plans for clients in the event an incident is detected. These plans are agreed upon by clients before PII is exchanged. These plans are also reviewed annually to ensure they comply with industry standards and best practices. |
| | **Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies). | In the event of an incident communications would be made to impacted clients as to the cause of the incident, what harm (if any) was done, mitigation steps underway/completed and an assessment of what went wrong and how an incident of this type will be prevented in the future. |
| | **Analysis (RS.AN):** Analysis is conducted to ensure effective response and support recovery activities. | If an incident occurs the Subcontractor is tasked with reviewing the incident, mitigation steps taken and prevention of future events. |
| | **Mitigation (RS.MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident. | The Subcontractor is contractually obligated with ensuring that if an incident is detected mitigation must begin immediately. |
| | **Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. | If an incident occurs NLP and the Subcontractor will review the incident from beginning to end to understand the incident, the response and what can be done to prevent incidents from occurring in the future. |
| 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 processes are maintained by the Subcontractor and can be implemented when necessary. These include full platform backups, data reintegration and post incident management. |
| | **Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities. | NLP and the Subcontractor meet monthly to discuss platform security and stability and examine industry best practices and policies to ensure that recovery efforts are up to date and determined if any changes are required. |
| | **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). | NLP and its Subcontractor work together on communication of (if necessary) recovery events to both internally and to external clients. These communications can include, direct email, web conferencing and in-platform communications. |