

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -**SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION**

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	<hr/>
PII Declaration	<p>Does your organization/software collect student personally identifiable information (PII) or staff PII?</p> <p>Examples of student PII:</p> <ul style="list-style-type: none">a. The student's name;b. The name of the student's parent or other family members;c. The address of the student or student's family;d. A personal identifier, such as the student's social security number, student number, or biometric record;e. Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name; <p>Examples of staff APPR PII:</p> <ul style="list-style-type: none">a. Teacher Id, Social Security Number, Employee Number, Biometric Recordb. Name, Mother's Maiden Name, Parent's Namec. Birthdate, Place of Birth, Addressd. Gender, Race, Salary <p><input type="checkbox"/> IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT.</p> <p>If you collect the PII information above, please complete the remainder of this form.</p>
Description of the purpose(s) for which Contractor will receive/access PII	
Type of PII that Contractor will receive/access	<p>Check all that apply:</p> <p><input type="checkbox"/> Student PII</p> <p><input type="checkbox"/> APPR PII</p>

Contract Term	Contract Start Date _____ Contract End Date _____
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" type="checkbox"/> Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) <input type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party. <input type="checkbox"/> Using Contractor owned and hosted solution <input type="checkbox"/> Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

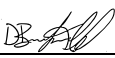
The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a 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.	
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	
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.	
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.	
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.	
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	
7	Describe your secure destruction practices and how certification will be provided to the EA.	
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	.

Western Suffolk BOCES Education Law §2-d Bill of Rights for Data Privacy and Security

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 or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("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, 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); and 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 at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to: dpo@wsboces.org. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 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 PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, 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.

CONTRACTOR	
[Signature]	
[Printed Name]	
[Title]	
Date:	

Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	We will implement applicable data and privacy contract requirements over the life of the Contract by first conducting a comprehensive assessment of the data and privacy needs specific to the contract. We then integrate industry-standard end-to-end encryption technologies for data in transit and at rest. Periodic vulnerability assessments and penetration testing would be performed to validate the efficacy of data security measures. All staff are given data privacy training and we conduct regular compliance audits. Breach notification processes exist as per legal requirements. Any amendments in laws during the contract period will be updated promptly.
Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	<p>Administrative Safeguards: We have established a privacy policy that dictates the use, access, and handling of PII. Regular training of staff members on data protection regulation is conducted and they are told about the importance of PII protection.</p> <p>Operational Safeguards: All access to PII is role-based, meaning only authorized individuals can access PII for defined purposes. Access logs are maintained and regularly audited. PII is anonymized or pseudonymized wherever possible.</p> <p>Technical Safeguards: PII is stored in encrypted form using up-to-date secure encryption algorithms. Firewalls, antivirus software and intrusion detection/prevention systems are in place. Data is backed up regularly and systems are in place for timely updates and patches.</p>
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.	All employees, officers, and subcontractors involved in delivering services under the Contract receive mandatory training on federal and state laws related to PII confidentiality. The training is carried out at the onset of their roles and is refreshed annually, or anytime significant legal changes occur. An emphasis is also laid on understanding the implications of non-compliance to these laws.
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.	Our contracting process with employees and subcontractors includes signing a contract detailing their responsibilities, roles, and obligations, including adherence to data protection and privacy provisions. We also require them to sign a non-disclosure agreement, committing to maintaining the confidentiality of sensitive information, including PII. Any violation of these agreements is subject to penalties as laid out in the contract. Regular audits are performed to ensure compliance.
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.	<p>Our system includes intrusion detection systems and continuous monitoring to detect any unauthorized access. When a breach is suspected, we promptly notify the relevant authorities, including the EA, about the nature and extent of the breach. Simultaneously, we begin an internal investigation.</p> <p>We are committed to not only addressing the breach but also taking necessary actions to prevent its recurrence, by rectifying any vulnerability and strengthening the existing protection measures. Furthermore, in line with our commitment to transparency, we inform those individuals whose PII could be at risk.</p>
Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	When the data is no longer required to fulfill our contractual obligations, a secure and controlled data transition process begins. We generate a complete, decrypted data dump or transfer in the format agreed upon in the contract. The data is then securely transmitted to the EA. Once confirmation of successful receipt and data integrity is received from the EA, we then delete all the data from our systems.
Describe your secure destruction practices and how certification will be provided to the EA.	We use secure deletion methods to ensure that the deleted data cannot be recovered. However, we do not issue a certificate of deletion.
Outline how your data security and privacy program/practices align with the EA's applicable policies.	See above
NIST framework:	
Asset Management (ID.AM):	Ellii complies with the ID.AM requirement by maintaining a comprehensive, up-to-date inventory of all our data, personnel, devices, and systems. We conduct regular audit reviews to ensure the accuracy and completeness of this inventory. Moreover, the roles and responsibilities of managing these assets are clearly defined and communicated to our staff, following a need-to-know principle to restrict access and reduce risk.
Business Environment (ID.BE):	We regularly conduct reviews of our business environment which include detailed analysis of our mission, objectives, stakeholders, and activities. This understanding forms the basis of our cybersecurity policies and initiatives. Roles and responsibilities related to cybersecurity are clearly defined and are aligned with our business priorities. For risk management decisions, we employ a risk-based approach that takes into consideration the potential impact on our mission and objectives.
Governance (ID.GV):	Our company has a defined set of policies, procedures, and processes in place which are designed in compliance with regulatory, legal, risk, environmental, and operational requirements. We have a dedicated compliance team that is responsible for understanding these requirements and implementing the necessary processes.
Risk Assessment (ID.RA):	Our organization integrates risk assessment as a critical part of our cybersecurity management strategy. We employ a dedicated risk assessment team that regularly conducts comprehensive evaluations to understand potential cybersecurity risks, relating to the operations, assets, and personnel. This involves identifying and analyzing possible threats, vulnerabilities, their impact, and probability of occurrence, based on the guidance provided in NIST SP 800-30. The findings guide allocation of resources and decision-making in managing these cybersecurity threats, and are documented, regularly updated, and communicated to management and relevant stakeholders to ensure awareness and strategic response company-wide.
Risk Management Strategy (ID.RM):	In compliance with the ID.RM requirement, Ellii establishes clear priorities, constraints, risk tolerances, and assumptions, and uses them to inform all operational risk decisions. These guidelines are crafted through collaboration between our risk management team and key business stakeholders.
Supply Chain Risk Management (ID.SC):	We have clearly defined our priorities, constraints, risk tolerances, and assumptions related to supply chain risk, which guide our risk decisions in this area. This includes rigorous vetting of all 3rd party services and subcontractors for compliance with our security standards before onboarding and regular compliance checks afterwards. We use various tools and risk assessment methodologies to identify, analyze, and manage potential risks in the supply chain. This includes risks related to data security, reliability of services provided by 3rd party applications, or instability in their business operations.

Identity Management, Authentication and Access Control (PR.AC):	We employ strong identity and access management (IAM) practices, ensuring individuals have access to only those resources that are required for their roles. This is managed through a robust Role-Based Access Control system. Access to both physical and logical assets and associated facilities is strictly limited to authorized users, processes, and devices.
Awareness and Training (PR.AT):	Ellii values the importance of cybersecurity awareness and training (PR.AT) and has implemented an internal program to ensure it. All personnel and partners are provided with ongoing cybersecurity awareness education. This includes training on cyber threats, safe online conduct, and our organization's cybersecurity policies and procedures.
Data Security (PR.DS):	We comply with this requirement through the implementation of various data safeguards. Firstly, we utilize encryption for data both at rest and in transit to maintain confidentiality and integrity. Secondly, we regularly conduct risk assessments to understand and mitigate potential threats. We also restrict access to sensitive data on a 'need-to-know basis', utilizing Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) for additional security. Furthermore, our company keeps up-to-date backups of essential data and employs data loss prevention strategies to maintain availability. All these procedures are continually reviewed and updated according to our risk management strategy.
Information Protection Processes and Procedures (PR.IP):	At Ellii, we have a comprehensive set of security policies and procedures that clearly outline the purpose, scope, roles, responsibilities, along with the management commitment. These policies include the acceptable use of systems, incident response plans, disaster recovery plans, and more. Regular audits are conducted to confirm compliance, and any lapses or discrepancies are reported and corrected immediately. These policies are also reviewed and updated regularly to reflect changing threats, business requirements, and technological advances. Additionally, we focus on awareness and training programs to ensure all employees understand their roles in protecting information systems and assets. We work to foster a security-conscious culture within the organization.
Maintenance (PR.MA):	We have clear procedures for handling system malfunctions and bugs on our software. Our hardware is maintained by reliable partners such as AWS and Heroku, who have data centers, physical infrastructure and operations that have been accredited under ISO 27001, SOC 1, and SOC 2.
Protective Technology (PR.PT):	Our protective measures include the use of firewalls, intrusion detection systems, antivirus software, and encryption methods. These solutions are continuously monitored and managed to ensure their effectiveness. We conduct periodic security audits and vulnerability assessments to identify any potential weaknesses and update our security solutions accordingly. Additionally, we have established Service Level Agreements (SLAs) with vendors to ensure they provide the necessary security measures and comply with our policies and procedures.
Anomalies and Events (DE.AE):	The Ellii Engineering Team has implemented comprehensive network monitoring and intrusion detection systems that help detect any anomalous activity within our infrastructure. We use analytics tools to understand normal system behavior and to flag deviations from these patterns as anomalies. Whenever an anomaly or event is detected, automatic alerts are sent to our dedicated cybersecurity team for immediate analysis to determine the potential impact. We also keep detailed logs of all system activity for forensic purposes and to help with the identification and rectification of potential weaknesses. In addition, regular system health checks are performed to look for unexpected changes, and continuous network scans are done to detect unfamiliar devices or unwanted traffic. All these approaches help us in proactive detection and quicker incident response.
Security Continuous Monitoring (DE.CM):	We employ continuous monitoring procedures to proactively detect potential cybersecurity events and to validate the effectiveness of our protective measures. These processes include real-time network surveillance, periodic system and application audits, and the active tracking of user actions for anomalous behavior.
Detection Processes (DE.DP):	Our procedures involve identification, classification, and prioritization of anomalies, alerting the relevant staff, and taking timely action to mitigate potential threats. We also keep our detection processes updated by incorporating the latest threat intelligence, lessons learned from past incidents, and insights from industry best practices. This ensures our detection mechanisms remain fine-tuned to respond effectively to the ever-evolving threat landscape.
Response Planning (RS.RP):	We are working towards having a robust Incident Response Plan (IRP) that clearly outlines the steps to be taken when a cybersecurity incident is detected. This includes roles and responsibilities, communication protocols, steps for containment, eradication, recovery, and follow-up actions. Our security team is being trained to execute this plan under various types of potential cybersecurity incidents. All incidents are logged, analyzed, and documented in detail for future reference and to improve our response to similar events.
Communications (RS.CO):	Ellii firmly believes in the importance of coordinated communication during a cybersecurity response. As part of our Response Plan, we are designing protocols for timely communication with all relevant internal stakeholders such as IT, HR, legal, and public relations teams. When necessary, we also collaborate with external stakeholders such as law enforcement, regulatory bodies, cybersecurity consultants, and law firms. We have established communication plans with these entities to ensure efficient coordination. Also, we comply with all laws and regulations regarding breach notifications to affected parties and public disclosure. All communications are done in a manner that is transparent but does not compromise any further aspects of our security or ongoing investigative efforts.
Analysis (RS.AN):	We conduct thorough analysis post any cybersecurity incidents. We analyze the incident's root cause, entry points, affected systems, data compromised, and the effectiveness of our response. This helps us understand how the incident occurred, how well our response measures worked, and where improvements can be made. This analysis spans technical forensic investigations, procedural evaluations, and a review of the human factors involved. The findings are used to strengthen our security policies, improve our incident response process, and avoid similar incidents in the future. We also believe in knowledge sharing and hence, lessons learned from this analysis are shared with relevant teams within the organization through briefings and training. These activities support our ultimate aim of continuous improvement in our cybersecurity posture.

Mitigation (RS.MI):	Upon detection of an event, our first step is to contain the incident to prevent its spread. This could involve isolating affected systems or blocking malicious IP addresses. Simultaneously, we perform immediate actions to mitigate the effects of the incident such as revoking unauthorized access, repairing system vulnerabilities, or restoring lost data from backups. Upon containment and mitigation, our focus shifts to fully resolving the incident, eradicating the threat from our system, and returning to normal operations. Any system affected by the incident is deeply analyzed to remove any residual threats, patched, and thoroughly tested before being returned to the operational environment.
Improvements (RS.IM):	After every incident, a post-incident review is conducted to analyze what happened, what worked well, what didn't, and what can be improved. We thoroughly document the findings and convert them into actionable improvements for our security protocol, response strategies, and training initiatives. These lessons learned are not only limited to incidents within our organization. We also study cybersecurity incidents in the wider industry and incorporate relevant lessons into our response and detection strategies. By doing this, our cybersecurity approach evolves continuously, always staying updated with new threats and best practices.
Recovery Planning (RC.RP):	In the case of a cybersecurity incident, we are prepared to quickly restore all systems or assets affected. This plan involves defined processes and procedures, such as restoring from backups, rebuilding systems, and validating the security of restored systems. We also ensure regular backups of critical data and systems and we test the recovery procedures periodically to ensure quick and efficient recovery when needed.
Improvements (RC.IM):	After each recovery operation, our company conducts a thorough review to learn from the experience. This includes understanding what aspects of the recovery worked well, what didn't, and where improvements can be made. These lessons learned are then shared with the relevant teams and used to update our recovery planning and processes. This continuous improvement mindset keeps our recovery strategies effective and up-to-date. For instance, if a recovery process takes longer than expected, we identify the bottlenecks and work on strategies to streamline the process for future incidents. Therefore, by incorporating these lessons learned, we ensure more efficient and effective recovery efforts moving forward.
Communications (RC.CO):	Our recovery process includes clear communication protocols with both internal and external parties. Internally, we provide regular updates to relevant teams about recovery progress and any impact on business operations. Externally, we are proactive in communicating with Internet Service Providers, vendors, and when necessary, the owners of attacking systems to mitigate the problem at its source. If our customers are affected, we send out timely notifications about the incident and the steps we are taking to resolve it.