

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> |
| 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> <ul style="list-style-type: none"><input type="checkbox"/> Student PII<input type="checkbox"/> APPR PII |

| | |
|--|---|
| 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 type="checkbox"/> Contractor will utilize subcontractors. |
| Data Transition and Secure Destruction | Upon expiration or termination of the Contract, and EA's written request , 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 30 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 | |

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 <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. | Aligned. MH utilizes centralized systems such as CMDB and WorkDay to manage personnel and systems. |
| | 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. | Aligned. |
| | 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. | Aligned. |
| | Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. | Aligned. MH has a centralized Cybersecurity function responsible for the security of the entire enterprise and its multifaceted operations. |
| | Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. | Aligned. |
| | Supply Chain Risk Management (ID.SC): The organization’s priorities, constraints, risk tolerances, and assumptions are | Aligned. |

| Function | Category | Contractor Response |
|----------------------------|---|---|
| | <p>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>PROTECT (PR)</p> | <p>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.</p> | <p>Aligned. MH practices Role-Based Access Control (RBAC) and Principle of Least Privilege (PoLP) on all critical systems and facilities. All access is centrally logged and monitored 24x7.</p> |
| | <p>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.</p> | <p>Aligned. Cybersecurity attestations are performed annually; awareness and training sessions are performed enterprise-wide more frequently throughout the year.</p> <p>For the Cybersecurity Team specifically, annual training and certifications are obtained in order to increase skillset and maintain CSPs. Many members on the Cybersecurity Team are SANS certified.</p> |
| | <p>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.</p> | <p>Aligned.</p> |
| | <p>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.</p> | <p>Aligned. All security policies and standards are posted internally.</p> |
| | <p>Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.</p> | <p>Aligned.</p> |
| | <p>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.</p> | <p>Aligned.</p> |

| Function | Category | Contractor Response |
|-----------------|--|---|
| DETECT (DE) | Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood. | Aligned. Anomalous activity is still investigated in the event it correlates with other events within the environment. |
| | Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. | Aligned. Security events are monitored 24x7 by our onshore and offshore Security Operations Center (SOC). |
| | Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. | Aligned. Standard Operating Procedures are in place for each alert type. |
| RESPOND (RS) | Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents. | Aligned. Standard Operating Procedures are in place with SLAs and the overall detailed process. |
| | Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies). | Aligned. |
| | Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities. | Aligned. |
| | Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident. | Aligned. Standard Operating Procedures are in place which include steps for containment. |
| | Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. | Aligned. Lessons learned are documented and incorporated into SOPs. |
| 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. | Aligned. Standard Operating Procedures are in place with SLAs and the overall detailed process. |
| | Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities. | Aligned. |
| | Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating | Aligned. |

| Function | Category | Contractor Response |
|----------|--|---------------------|
| | centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors). | |

Exhibit C.2

McGraw Hill LLC Data Privacy and Security Guidelines

This Data Privacy and Security Guidelines (“**DPSG**” or “**Security Guidelines**”) document sets forth the duties and obligations of McGraw Hill (defined below) with respect to Personal Information (defined below). In the event of any inconsistencies between the DPSG and the Agreement (defined below), the parties agree that the DPSG will supersede and prevail. Capitalized terms not defined herein shall have the meaning ascribed to them in the Agreement.

1. Definitions.

- a. **"Agreement"** means the Agreement for the Services between the McGraw Hill LLC entity (“**McGraw Hill**”) and Subscriber incorporating the [Privacy Notice](#) to which these Security Guidelines are referenced and made a part thereof.
- b. **"Applicable Laws"** means federal, state and international privacy, data protection and information security-related laws, rules and regulations applicable to the Services and to Personal Information.
- c. **"End User Data"** means the data provided to or collected by McGraw Hill in connection with McGraw Hill’s obligations to provide the Services under the Agreement.
- d. **"Personal Information"** means information provided to McGraw Hill in connection with McGraw Hill’s obligations to provide the Services under the Agreement that (i) could reasonably identify the individual to whom such information pertains, such as name, address and/or telephone number or (ii) can be used to authenticate that individual, such as passwords, unique identification numbers or answers to security questions or (iii) is protected under Applicable Laws. For the avoidance of doubt, Personal Information does not include aggregate, anonymized data derived from an identified or identifiable individual.
- e. **"Processing of Personal Information"** means any operation or set of operations which is performed upon Personal Information, such as collection, recording, organization, storage, use, retrieval, transmission, erasure or destruction.
- f. **"Third Party"** means any entity (including, without limitation, any affiliate, subsidiary and parent of McGraw Hill) that is acting on behalf of, and is authorized by, McGraw Hill to receive and use Personal Information in connection with McGraw Hill’s obligations to provide the Services.
- g. **"Security Incident"** means the unlawful access to, acquisition of, disclosure of, loss, or use of Personal Information.
- h. **"Services"** means any services and/or products provided by McGraw Hill in accordance with the Agreement.

2. Confidentiality and Non-Use; Consents.

- a. McGraw Hill agrees that the Personal Information is the Confidential Information of Subscriber and, unless authorized in writing by Subscriber or as otherwise specified in the Agreement or this DPSG, McGraw Hill shall not Process Personal Information for any purpose other than as reasonably necessary to provide the Services, to exercise any rights granted to it under the Agreement, or as required by Applicable Laws.
- b. McGraw Hill shall maintain Personal Information confidential, in accordance with the terms set forth in this Security Guidelines and Applicable Laws. McGraw Hill shall require all of its employees authorized by McGraw Hill to access

Personal Information and all Third Parties to comply with (i) limitations consistent with the foregoing, and (ii) all Applicable Laws.

- c. Subscriber represents and warrants that in connection with any Personal Information provided directly by Subscriber to McGraw Hill, Subscriber shall be solely responsible for (i) notifying End Users that McGraw Hill will Process their Personal Information in order to provide the Services and (ii) obtaining all consents and/or approvals required by Applicable Laws.

3. Data Security.

McGraw Hill shall use commercially reasonable administrative, technical and physical safeguards designed to protect the security, integrity, and confidentiality of Personal Information. McGraw Hill's security measures include the following:

- a. Access to Personal Information is restricted solely to McGraw Hill's staff who need such access to carry out the responsibilities of McGraw Hill under the Agreement.
- b. Access to computer applications and Personal Information are managed through appropriate user ID/password procedures.
- c. Access to Personal Information is restricted solely to Subscriber personnel based on the user role they are assigned in the system (provided, however, that it is the Subscriber's responsibility to ensure that user roles match the level of access allowed for personnel and that their personnel comply with Applicable Law in connection with use of such Personal Information).
- d. Data is encrypted in transmission (including via web interface) and at rest at no less than 256-bit level encryption.
- e. McGraw Hill or a McGraw Hill authorized party performs a security scan of the application, computer systems and network housing Personal Information using a commercially available security scanning system on a periodic basis.

4. Data Security Breach.

- a. In the event of a confirmed Security Incident, McGraw Hill shall (i) investigate the Security Incident, identify the impact of the Security Incident and take commercially reasonable actions to mitigate the effects of any such Security Incident, (ii) timely provide any notifications to Subscriber or individuals affected by the Security Incident that McGraw Hill is required by law, subject to applicable confidentiality obligations and to the extent allowed and/or required by and not prohibited by Applicable Laws or law enforcement.
- b. Except to the extent prohibited by Applicable Laws or law enforcement, McGraw Hill shall, upon Subscriber's written request and to the extent available, provide Subscriber with a description of the Security Incident and the type of data that was the subject of the Security Incident.

5. Security Questionnaire.

Upon written request by Subscriber, which request shall be no more frequently than once per twelve (12) month period, McGraw Hill shall respond to security questionnaires provided by Subscriber, with regard to McGraw Hill's information security program applicable to the Services, provided that such information is available in the ordinary course of business for McGraw Hill and it is not subject to any restrictions pursuant to McGraw Hill's privacy or data protection or information security-related policies or standards. Disclosure of any such information shall not compromise McGraw Hill's confidentiality obligations and/or legal obligations or privileges. Additionally, in no event shall McGraw Hill be required to make any disclosures prohibited by Applicable Laws. All the information provided to Subscriber under this section shall be Confidential Information of McGraw Hill and shall be treated as such by the Subscriber.

6. Security Audit.

Upon written request by Subscriber, which request shall be no more frequently than once per twelve (12) month period, McGraw Hill's data security measures may be reviewed by Subscriber through an informal audit of policies and procedures or through an independent auditor's inspection of security methods used within McGraw Hill's infrastructure, storage, and other physical security, any such audit to be at Subscriber's sole expense and subject to a mutually agreeable confidentiality agreement and at mutually agreeable timing, or, alternatively, McGraw Hill may provide Subscriber with a copy of any third party audit that McGraw Hill may have commissioned.

7. Records Retention and Disposal.

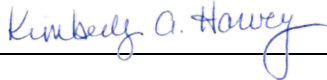
- a. Subscriber may access, correct, and delete any Personal Information in McGraw Hill's possession by submitting McGraw Hill's Personal Information Request Form: <https://www.mheducation.com/privacy/privacy-request-form>.
- b. McGraw Hill will use commercially reasonable efforts to retain End User Data in accordance with McGraw Hill's End User Data retention policies.

McGraw Hill will use commercially reasonable efforts to regularly back up the Subscriber and End User Data and retain any such backup copies for a minimum of 12 months.

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: | |

March 12, 2024