McGraw-Hill Education Data Security Policy – Louisiana State

This Data Security Policy Agreement (**"Data Security Policy"** or **"DPSA"**) sets forth MHE's duties and obligations with respect to Personally Identifiable Information (defined below). In the event of any inconsistencies between the Data Security Policy and the Agreement (defined below), the parties agree that the Data Security Policy will supersede and prevail. Capitalized Terms not defined herein shall have the meaning ascribed to them in the agreement.

1. **Definitions.**
   a. **"Agreement"** means any Agreement between McGraw-Hill Global Education Holdings, LLC and Subscriber, which this DPSA is hereby incorporated into 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 Personally Identifiable Information.
   c. **"End User Data"** means the data provided to or collected by MHE in connection with MHE's obligations to provide the Services under the Agreement.
   d. **"Personally Identifiable Information"** or **"PII"** means information provided to MHE in connection with MHE's obligations to provide the Services under the Agreement that when used on its own or with other information (i) could reasonably identify, contact, or locate 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, PII does not include aggregate, anonymized data derived from an identified or identifiable individual.
   e. **"Processing of PII"** means any operation or set of operations which is performed upon PII, 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 MHE) that is acting on behalf of, and is authorized by, MHE to receive and use PII in connection with MHE's obligations to provide the Services.
   g. **"Security Incident"** means the unlawful access to, acquisition of, disclosure of, loss, or use of PII.
   h. **"Services"** means any services and/or products provided by MHE in accordance with the Agreement.

2. **Privacy Compliance Standards; Confidentiality and Non-Use; Consents.**
   a. MHE agrees that the PII is the Confidential Information of Subscriber and MHE shall only Process PII as reasonably necessary to provide the Services as described in the Agreement, to exercise any rights granted to it under the Agreement, or as required by Applicable Laws.
   b. MHE shall maintain PII confidential, in accordance with the terms set forth in this DPSA and Applicable Laws. MHE shall require all of its employees authorized by MHE to access PII 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 PII provided directly by Subscriber to MHE, Subscriber shall be solely responsible for (i) notifying End Users that MHE will Process their PII in order to provide the Services and (ii) obtaining all consents and/or approvals required by Applicable Laws.
   d. No PII at any time will be processed on or transferred to any portable computing device or portable storage medium, unless such portable device or medium is owned by MHE and is encrypted so that no unauthorized person shall be able to access any data or information stored

on the device. MHE shall exercise the appropriate level of care in its handling and use of portable devices and storage mediums that contains PII. MHE shall maintain responsibility for such devices.

3. **Access, Authentication and Data Security**. MHE shall use commercially reasonable administrative, technical and physical safeguards designed to protect the security, integrity, and confidentiality of PII. MHE's security measures include the following:
   a. Access to PII is restricted solely to MHE's staff who need such access to carry out the responsibilities of MHE under the Agreement;
   b. Access to computer applications and PII are managed through appropriate user ID/password procedures;
   c. Access to PII 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 PII);
   d. Data is encrypted in transmission (including via web interface) at no less than 128-bit level encryption; and
   e. MHE or an MHE authorized party performs a security scan of the application, computer systems and network housing PII using a commercially available security scanning system on an annual basis.

4. **Breach Planning/Notification/Remediation**.
   a. In the event of a Security Incident , MHE 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 individuals affected by the Security Incident that MHE is required to provide, and, (iii) notify Subscriber of the Security Incident, subject to applicable confidentiality obligations and to the extent allowed and/or required by Applicable Laws.
   b. Except to the extent prohibited by Applicable Laws, MHE shall, upon Subscriber's written request, provide Subscriber with a description of the Security Incident and the type of data that was the subject of the Security Incident.
   c. MHE agrees to comply with the Louisiana Database Breach Notification Law (Act 499) and all applicable laws that require the notification of individuals in the event of MHE's unauthorized release of PII. In the event of MHE's breach of any of MHE's security obligations requiring MHE notification under applicable law, MHE agrees to notify Subscriber, subject to applicable confidentiality obligations and to the extent allowed and/or required by applicable law and will work with Subscriber to inform all affected individuals in accordance with applicable law and to indemnify, hold harmless and defend Subscriber and its employees from and against any claims, damages, or other harm arising out of any claim that MHE failed to notify following a MHE act or omission pursuant to this paragraph or failed to comply with any of MHE's obligations contained within this DPSA.

5. **Security Questionnaire**. Upon written request by Subscriber, which request shall be no more frequently than once per twelve (12) month period, MHE shall respond to security questionnaires provided by Subscriber, with regard to MHE's information security program applicable to the Services, provided that such information is available in the ordinary course of business for MHE and it is not subject to any restrictions pursuant to MHE's privacy or data protection or information security-related policies or standards. Disclosure of any such information shall not compromise