3rd Millennium Classrooms
Data Breach Notification Policy

1. Purpose.

3rd Millennium Classrooms, a Texas-based business, is committed to providing privacy protection for our employees and students by complying with all relevant data protection laws. This Policy clearly defines and outlines our data breach notification protocols. The Policy is meant to ensure that 3rd Millennium Classrooms is in compliance with Texas laws regarding data security, specifically Tex. Bus. & Com. Code §§ 521.002, 521.053.

2. Scope.

The users of this document are customers, employees, contractors, and other partners of 3rd Millennium Classrooms. This Policy shall be provided to anyone who provides sensitive personal information to us.

3. Definitions.

3.1 Security Breach. Any unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal maintained by an entity, including data that is encrypted if the person accessing the data has the key required to decrypt the data.

3.2 Sensitive Personal Information. An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted: Social Security Number; Driver license number or government-issued ID number; or Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

4. Notification.

4.1 Notification Obligation.

4.1.1 Any entity that maintains computerized data that includes sensitive personal information that the entity does not own shall notify the owner or license holder of

the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

4.1.2 Any entity to which the Texas statute applies shall disclose any breach of system security, after discovering or receiving notification of the breach, to any person, including nonresidents, whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

4.2 Notification Timing.

4.2.1 If a data breach is suspected or confirmed, a disclosure shall be made as quickly as possible, consistent with the legitimate needs of law enforcement or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

4.3 Notification Procedure.

4.3.1 3rd Millennium Classrooms uses Rackspace to store customer sensitive personal information. You can review their privacy policy here: https://www.rackspace.com/information/legal/privacystatement.

4.3.2 Upon receiving information notification from Rackspace that sensitive personal information may have been exposed following a data breach, we will notify those victims affected immediately and without delay.

4.3.2.1 Notice of a suspected or confirmed data breach may be provided by way of written notice at the last known address of those affected or by electronic notice (as consistent with the E-Sign Act, 15 U.S.C. § 7001). If those victims affected by a data breach are residents of a state with its own breach notification requirement, we may provide notice under that state's law.

4.3.3 The CEO and Data Protection Officer of 3rd Millennium Classrooms, Katie Church, will chair an incident response team to handle the breach or exposure. An incident response team may include an IT officer, a legal compliance officer, and a human resources officer. The incident response team will analyze details the breach in order to determine the severity of the exposure. The team will also be responsible for minimizing the impact of exposure of those victims affected.

5. Ownership and Responsibilities.

5.1 Data Protection Officer. The Data Protection Officer of 3rd Millennium Classrooms, Katie Church, is responsible for managing records associated with data breach notification policy, providing oversight and coordination of security systems and

procedures, and facilitating communications between the incident response team and those victims affected by a data breach.

5.2 IT Officer. The IT Officer of 3rd Millennium Classrooms is responsible for communicating with third-party partners to determine the cause, extent, and resolution of the breach. The IT Officer is also responsible for checking IT systems for additional breaches. The IT Officer should provide records of potential or confirmed risks to the Data Protection Officer.

5.3 Legal Compliance Officer. The Legal Compliance Officer is responsible for notifying governmental, or other authorities, of data breaches.

5.4 Human Resources Officer. The Human Resources Officer is responsible for facilitating communications between 3rd Millennium Classrooms and those victims affected by a data breach.

6. Enforcement.

Any personnel that violates this policy, through omission or action, may be subject to disciplinary action, including termination of employment. Any third-party partner in violation of this policy, through omission or action, may have their connection to 3rd Millennium Classrooms terminated.

7. Managing Records.

This document is valid as of the date listed below.

The owner of this document is the Data Protection Officer, who is responsible for updating this document once per year and notifying staff of any relevant changes.

Version:	1
Date of Version:	May 29, 2019
Created by:	
Approved by:	
Confidentiality Level:	PUBLIC

_____

_____

Data Protection Officer Signature Date