CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

Version 1.0

Lodi Unified School District

and

SyTech Solutions

This California Student Data Privacy Agreement ("DPA") is entered into by and between the
Lodi Unified School District (hereinafter referred to as "LEA") and
SyTech Solutions (hereinafter referred to as "Provider") on July 1, 2017 .
The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated July 1, 2017 ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive and the LEA may provide documents or data that are covered by several federal and statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232 h; and

WHEREAS, the documents and data transferred from California LEAs are also subject to several California student privacy laws, including AB 1584, found at California Education Code Section 49073.1 and the Student Online Personal Information Protection Act (sometimes referred to as either "SB 1177" or "SOPIPA") found at California Business and Professions Code section 22584; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms", agrees to allow other LEAs in California the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from the LEA pursuant to the Service Agreement, including compliance with all applicable privacy statutes, including the FERPA, PPRA, COPPA, SB 1177 (SOPIPA), and AB 1584. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA. Control duties are set forth below.

2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational services described below and as may be further outlined in Exhibit "A" hereto:

3. **Student Data to Be Provided**. In order to perform the Services described in the Service Agreement, LEA shall provide the categories of data described below or as indicated in the Schedule of Data, attached hereto as Exhibit "B":

4. **DPA Definitions**. The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over term used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data or any other Pupil Records transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Parties agree that as between them all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of student data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner to the LEA's request for personally identifiable information in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. Provider shall, at the request of the LEA, transfer Student generated content to a separate student account.

4. **Third Party Request**. Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party unless legally prohibited.

5. **No Unauthorized Use**. Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in the Service Agreement.

6. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree protect Student Data in manner consistent with the terms of this DPA

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With FERPA**. LEA shall provide data for the purposes of the Service Agreement in compliance with the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. section 1232 g, AB 1584 and the other privacy statutes quoted in this DPA.

2. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

3. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

4. **District Representative**. At request of Provider, LEA shall designate an employee or agent of the District as the District representative for the coordination and fulfillment of the duties of this DPA.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all California and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, AB 1584, and SOPIPA.

2. **Authorized Use**. The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above.

3. **Employee Obligation**. Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of FERPA laws with respect to the data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure**. Provider shall not disclose any data obtained under the Service Agreement in a manner that could identify an individual student to any other entity in published results of studies as authorized by the Service Agreement. Deidentified information may be used by the vendor for the purposes of development and improvement of educational sites, services, or applications.

5. **Disposition of Data**. Provider shall dispose of all personally identifiable data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA's designee within 60 days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Provider shall provide written notification to LEA when the Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

6. **Advertising Prohibition**. Provider is prohibited from using Student Data to conduct or assist targeted advertising directed at students or their families/guardians. This prohibition includes the development of a profile of a student, or their families/guardians or group, for any commercial purpose other than providing the service to client. This shall not prohibit Providers from using data to make product or service recommendations to LEA.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to abide by and maintain adequate data security measures to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in in Exhibit "D" hereto. These measures shall include, but are not limited to:

    a. **Passwords and Employee Access.** Provider shall make best efforts practices to secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. As stated elsewhere in this DPA, employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall pass criminal background checks.

    b. **Destruction of Data.** Provider shall destroy all personally identifiable data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonable agree. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

c. **Security Protocols**. Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.

d. **Employee Training**. The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

e. **Security Technology**. When the service is accessed using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology protects information, using both server authentication and data encryption to help ensure that data are safe secure only to authorized users. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.

f. **Security Coordinator**. Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement

g. **Subprocessors Bound**. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

2. **Data Breach**. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident. Provider shall follow the following process:

a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

i. The name and contact information of the reporting LEA subject to this section.

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

c. At LEA's discretion, the security breach notification may also include any of the following:

i. Information about what the agency has done to protect individuals whose information has been breached.

ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

d. Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. Provider shall assist LEA in these efforts.

e. At the request and with the assistance of the District, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

ARTICLE VI: GENERAL OFFER OF PRIVACY TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms ("General Offer"), (attached hereto as Exhibit "E"), be bound by the terms of this DPA to any other LEA who signs the Acceptance on said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for no less than three (3) years.

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated.

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall

destroy all of LEA's data pursuant to Article V, section 1(b).

4. **Priority of Agreements**. This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA and AB 1584. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the addresses set forth herein.

6. **Application of Agreement to Other Agencies**. Provider may agree by signing the General Offer of Privacy Terms be bound by the terms of this DPA for the services described therein for any Successor Agency who signs a Joinder to this DPA.

7. **Entire Agreement**. This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

8. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

9. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF CALIFORNIA,

WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS LOCATED IN San Joaquin COUNTY, CALIFORNIA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

[*Signature Page Follows*]

IN WITNESS WHEREOF, the parties have executed this California Student Data Privacy Agreement as of the last day noted below.

Lodi Unified School District

Signature: ________________ Date: 6-29-17

Printed Name: Tim Hern Title/Position: Chief Business Officer/Associate Superintendent

Signature: ________________ Date: 6/29/17

Printed Name: Jon Pritt Title/Position: Vice President

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

1DocStop Document Management Solution to include:
-secure log-in authentication via username & password
-ability to capture paper and electronic records
-ability to index paper and electronic records
-ability to save, print & email records
-server to client communication encryption using secure server certificates (128-bit)
-systematic backups of data
-unlimited file storage
-unlimited user access
-system maintenance and software updates
-technical support

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc	✓
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	X
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Category of Data	**Elements**	**Check if used by your system**
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	

Category of Data	Elements	Check if used by your system
Other	Other student work data - Please specify:	
Transcript	Student course grades	X
	Student course data	X
	Student course grades/performance scores	X
	Other transcript data -Please specify:	Scanned Images

Category of Data	Elements	Check if used by your system
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data - Please specify:	
Other	Please list each additional data element used, stored or collected by your application	Scanned Images

EXHIBIT "C"

DEFINITIONS

AB 1584, Buchanan: The statutory designation for what is now California Education Code § 49073.1, relating to pupil records.

De-Identifiable Information (DII): De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

NIST 800-63-3: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

Operator: For the purposes of SB 1177, SOPIPA, the term "operator" means the operator of an Internet Website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Service Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in AB 1584.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes, without limitation, at least the following:

First and Last Name
Telephone Number
Discipline Records
Special Education Data
Grades
Criminal Records
Health Records
Biometric Information
Socioeconomic Information
Political Affiliations
Text Messages
Student Identifiers
Photos
Videos

Home Address
Email Address
Test Results
Juvenile Dependency Records
Evaluations
Medical Records
Social Security Number
Disabilities
Food Purchases
Religious Information
Documents
Search Activity
Voice Recordings

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student's Educational Record

Information in the Student's Email

Provider: For purposes of the Service Agreement, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. Within the Service Agreement the term "Provider" replaces the term "Third Party as defined in California Education Code § 49073.1 (AB 1584, Buchanan), and replaces the term as "Operator" as defined in SB 1177, SOPIPA.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational LEA employee.

SB 1177, SOPIPA: Once passed, the requirements of SB 1177, SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

School Official: For the purposes of this Agreement and pursuant to CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of California and Federal laws and regulations. Student Data as specified in <u>Exhibit B</u> is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subscribing LEA: An LEA that was not party to the original Services Agreement and who accepts the Provider's General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII. This term shall also include in it meaning the term "Service Provider," as it is found in SOPIPA.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Third Party: The term "Third Party" as appears in California Education Code § 49073.1 (AB 1584, Buchanan) means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DATA SECURITY REQUIREMENTS

See 1DocStop & Microsoft Azure Security &
Privacy Details and EDUCATION 1DOCSTOP HOSTING ADDENDUM

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Lodi Unified School District and which is dated 7/1/2017 to any other LEA ("Subscribing LEA") to anywho accepts this General Offer though its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the other LEA may also agree to change the data provided by LEA to the Provider to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify the California Student Privacy Alliance in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

SyTech Solutions

Signature: ______________________ Date: 6-29-17

Printed Name: Jon PRITT Title/Position: Vice President

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

LEA: ______________________

Signature: ______________________ Date: ______________________

Printed Name: ______________________ Title/Position ______________________

SyTech
SOLUTIONS

1DocStop & Microsoft Azure Security & Privacy Details

Microsoft partners with SyTech Solutions to ensure that 1DocStop complies with a wide range of international, country, state and industry-specific regulatory requirements (including HIPAA, FERPA California Education Code Section 49073.1).

Independently verified

By providing SyTech with compliant, independently verified cloud services, Microsoft makes it easy to achieve compliance for the infrastructure and applications, such as 1DocStop, that is run in Azure. Microsoft provides Azure customers with detailed information about its security and compliance programs, including audit reports and compliance packages, to help customers assess its services against their own legal and regulatory requirements.

In addition, Microsoft has developed an extensible compliance framework that enables it to design and build services using a single set of controls to speed up and simplify compliance across a diverse set of regulations and rapidly adapt to changes in the regulatory landscape. More information on specific compliance programs is available here:

- **ISO 27001/27002**
- **SOC 1/SSAE 16/ISAE 3402 and SOC 2**
- **Cloud Security Alliance CCM**
- **FERPA**
- **HIPAA**
- **FedRAMP**
- **FISMA**
- **FBI CJIS (Azure Government)**
- **PCI DSS Level 1**
- **United Kingdom G-Cloud**
- **Australian Government IRAP**
- **Singapore MTCS Standard**
- **EU Model Clauses**
- **Food and Drug Administration 21 CFR Part 11**
- **FIPS 140-2**

ISO 27001/27002 Audit and Certification

Azure is committed to annual certification against ISO/IEC 27001/27002:2013, a broad international information security standard. The ISO/IEC 27001/27002:2013 certificate validates that Microsoft has implemented the internationally recognized information security controls defined in this standard, including guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization.

The audit included the Information Security Management System (ISMS) for Azure, encompassing infrastructure, development, operations, management, support, and in-scope services. The certificate issued by the British Standards Institution (BSI) is publically available.

Additionally, Microsoft Azure services have incorporated the controls that embody ISO/IEC 27018 – an extension of the ISO 27001 standard with a code of practice governing the processing of personal information by cloud service providers. ISO 27018 provides controls that reflect considerations specifically for protecting personally identifiable information in public cloud services. For example, the ISO 27018 controls prohibit the use of customer data for advertising and marketing purposes without the customer's express consent. ISO 27018 also provides clear guidance for cloud service providers for the return, transfer and/or secure disposal of personal information of customers leaving their service and requires the cloud service provider to identify any sub-processor before customers enter into a contract, and inform customers promptly of new sub-processors, to give customers an opportunity to object or terminate their agreement.

SOC 1/SSAE 16/ISAE 3402 and SOC 2 Attestations

Azure has been audited against the Service Organization Control (SOC) reporting framework for both **SOC 1 Type 2** and **SOC 2 Type 2**. Both reports are available to customers to meet a wide range of US and international auditing requirements.

The SOC 1 Type 2 audit report attests to the design and operating effectiveness of Azure controls. The SOC 2 Type 2 audit included a further examination of Azure controls related to security, availability, and confidentiality. Azure is audited annually to ensure that security controls are maintained.

Audits are conducted in accordance with the Statement on Standards for Attestation Engagements (SSAE) No. 16 put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements (ISAE) 3402 put forth by the International Auditing and Assurance Standards Board (IAASB). In addition, the SOC 2 Type 2 audit included an examination of the Cloud Controls Matrix (CCM) from the Cloud Security Alliance (CSA).

The audit included the Information Security Management System (ISMS) for Azure, encompassing infrastructure, development, operations, management, support, and in-scope services. Customers should contact Azure Support (or new customers can contact their account representative) to request a copy of the SOC 1 Type 2 and SOC 2 Type 2 reports for Azure.

Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is designed to provide fundamental security principles to guide cloud vendors and to assist prospective customers in assessing the overall security risk of a cloud provider. Detailed information about how Azure fulfills the security, privacy, compliance, and risk management requirements defined in the CCM version 1.2 is also published in the CSA's Security Trust and Assurance Registry (STAR). In addition, the Microsoft Approach to Cloud Transparency paper provides an overview of how Microsoft addresses various risk, governance, and information security frameworks and standards, including the CSA CCM v1.2.

Family Educational Rights and Privacy Act (FERPA)

FERPA is a Federal law that protects the privacy of student education records, and imposes requirements on U.S. educational organizations regarding the use and disclosure of student education records. Educational organizations can use Azure to process data, such as student education records, in compliance with FERPA. Microsoft agrees to use and disclosure restrictions imposed by FERPA, will only use Customer Data to provide organizations with the Azure service, and will not scan Customer Data for advertising purposes.

HIPAA Business Associate Agreement (BAA)

HIPAA and the HITECH Act are United States laws that apply to healthcare entities with access to patient information (called Protected Health Information, or PHI). In many circumstances, for a covered healthcare company to use a cloud service like Azure, the service provider must agree in a written agreement to adhere to certain security and privacy provisions set forth in HIPAA and the HITECH Act. To help customers comply with HIPAA and the HITECH Act, Microsoft offers a BAA to customers as a contract addendum. SyTech Solutions had executed this agreement and can provide it to clients upon request.

Federal Risk and Authorization Management Program (FedRAMP)

Azure has been granted a Provisional Authority to Operate (P-ATO) from the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) at a Moderate impact level based upon the FIPS 199 classification. Following a rigorous security review, the JAB approved a provisional authorization that an executive department or agency can leverage to issue a security authorization and an accompanying Authority to Operate (ATO). This will allow U.S. federal, state, and local governments to more rapidly realize the benefits of the cloud using Azure.

FedRAMP is a mandatory U.S. government program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services.

The FedRAMP audit included the Information Security Management System (ISMS) for Azure, encompassing infrastructure, development, operations, management, support, and in-scope services. Government agencies can request the Azure FedRAMP security package. Microsoft intends to pursue FedRAMP certification for Azure Government.

Federal Information Security Management Act (FISMA)

The Federal Information Security Management Act of 2002 was implemented to provide agencies the ability to document and implement information security programs within their operational systems.

Previously, cloud providers were required to undergo FISMA assessments by individual federal agencies. Azure received an ATO from the General Services Administration under FISMA. In 2011, the FedRAMP program was created and designed to streamline the process for cloud service providers and agencies and has replaced FISMA authorizations as the preferred approach to validating the security of cloud services.

The FISMA audit included the Information Security Management System (ISMS) for Azure, encompassing infrastructure, development, operations, management, support, and in-scope services. Government agencies can request the current Azure FedRAMP security package.

Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS)

Microsoft has reviewed the Azure Government policies and procedures to verify that it meets the requirements necessary for U.S. state and local agencies to use in-scope services to store and process Criminal Justice Information. Azure will contractually commit and sign the FBI CJIS security addendum, which commits Azure to the same requirements that law enforcement and public safety must meet. Azure continues to work with a variety of states to enter into additional CJIS Information Agreements, which provide additional information to law enforcement authorities about the nature of the services, and ensure appropriate background screening for operating personnel.

Payment Card Industry (PCI) Data Security Standards (DSS) Level 1

Azure is Level 1 compliant under the Payment Card Industry (PCI) Data Security Standards (DSS) as verified by an independent Qualified Security Assessor (QSA), allowing merchants to establish a secure cardholder environment and to achieve their own certification.

The PCI DSS is an information security standard designed to prevent fraud through increased controls around credit card data. PCI certification is required for all organizations that store, process or transmit payment cardholder data. Customers can reduce the complexity of their PCI DSS certification by using compliant Azure services.

The audit included the Information Security Management System (ISMS) for Azure, encompassing infrastructure, development, operations, management, support, and in-scope services. The Azure PCI Attestation of Compliance and Azure Customer PCI Guide are available for immediate download.

United Kingdom G-Cloud OFFICIAL Accreditation

Azure has received OFFICIAL accreditation from the UK Government Pan Government Accreditor. Azure is available on the G-cloud Framework and details can be found on the UK's Digital Marketplace.

The OFFICIAL rating benefits a broad range of UK Public Sector organizations, including Local and Regional Government, National Health Service (NHS) trusts and some central government bodies who hold or transact public sector data for business conducted at the OFFICIAL level of Security Classification. Details of the OFFICIAL accreditation can be found here and form part of the UK Government's Cloud Security Principles.

OFFICIAL accreditation covers the Azure in-scope services listed on the Azure Trust Center.

Australian Government Information Security Registered Assessors Program (IRAP)

Azure has been assessed against the **Australian Government Information Security Registered Assessors Program (IRAP)** and a **letter of compliance** has been issued for **in-scope services**. The IRAP assessment provides assurance for public sector customers (and the partners that serve them) that Microsoft has appropriate and effective security controls in place for the processing, storage and transmission of Unclassified Sensitive data within Microsoft Azure. Unclassified Sensitive data represents the majority of federal government, healthcare, education and state government data in Australia.

Multi-Tier Cloud Security Standard for Singapore (MTCS SS 584:2013)

Azure has achieved Level-1 certification with the **Multi-Tier Cloud Security Standard for Singapore (MTCS SS)**, a cloud security standard, developed under the Singapore Information Technology Standards Committee (ITSC) to provide businesses with greater clarity on the levels of security offered by different cloud service providers. The standard covers areas such as data retention, data sovereignty, data portability, liability, availability, business continuity, disaster recovery, and incident management.

A rigorous assessment was conducted by the MTCS Certifying Body and included Microsoft development, operations, support, and **in-scope services**.

EU Model Clauses

Microsoft offers customers E.U. Standard Contractual Clauses that provide additional contractual guarantees around transfers of personal data for **in-scope services**. Microsoft's implementation of the E.U. model clauses has been validated by European Union data protection authorities as being in line with the rigorous privacy standards that regulate international data transfers by companies operating in its member states. Microsoft is the first company to receive **joint approval** from the E.U.'s Article 29 Working Party for its strong contractual commitments to comply with E.U. privacy laws no matter where data is located.

Food and Drug Administration 21 CFR Part 11

The Food and Drug Administration Part 11 of Title 21 Code of Federal Regulations, Electronic Records; Electronic Signatures (21 CFR Part 11) applies to entities that maintain records or submit information to include records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in FDA regulations. Part 11 also applies to electronic records submitted to the Agency under the Federal Food, Drug, and Cosmetic Act (the Act) and the Public Health Service Act (the PHS Act).

Since Part 11 became effective in 1997, the Food and Drug Administration has publicly emphasized their intent and commitment to overcome unnecessary restrictions on the use of electronic technology, significant costs of compliance and barriers to innovation and technology advances that stand in the way of public health benefit. The Part 11 requirements for validation, audit trails, record retention, record copying, and legacy systems and others introduce potential barriers and restrictions especially for agencies working in constrained time, resource or emergent public health crisis.

Azure's deep partnership with customers and partners in public sector health and life sciences industry resulted in the Qualification Guideline for Microsoft Azure. Working with the Qualification Guideline, entities are able to demonstrate Azure services and execution fulfills Part 11 requirements.

The Azure platform components which are within scope of this review include: Cloud Services (Web, Worker and VM roles), Azure Storage (Blobs, Queues, and Tables), Networking (Traffic Manager, Virtual Network), and Virtual Machines.

Federal Information Processing Standard (FIPS)

The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information. The National Institutes of Standards and Technology (NIST) publishes the list of vendors with validated FIPS 140-1 and 140-2 cryptographic modules. Azure uses Microsoft cryptographic modules in the validated list published by NIST, enabling customers to configure and use Azure Virtual Network services in a way that helps meet their information encryption requirements.

Location of Customer Data

Microsoft currently operates Azure in data centers around the world. In this section, we address common customer inquiries about access and location of Customer Data.

- Customers may specify the geographic area(s) ("geos" and "regions") of the Microsoft datacenters in which Customer Data will be stored. Available geos and regions are shown below. Please see service availability by region.

GEO (PREVIOUSLY MAJOR REGION)	REGION (PREVIOUSLY SUB-REGION)
United States	East US (Virginia) East US 2 (Virginia) Central US (Iowa) West US (California) North Central US (Illinois) South Central US (Texas)

- Microsoft may transfer Customer Data within a geo (e.g., within Europe) for data redundancy or other purposes. For example, Azure replicates Blob and Table data between two regions within the same geo for enhanced data durability in case of a major data center disaster.
- Microsoft will not transfer Customer Data outside the geo(s) customer specifies (for example, from Europe to U.S. or from U.S. to Asia) except where necessary for Microsoft to provide customer support, troubleshoot the service, or comply with legal requirements; or where customer configures the account to enable such transfer of Customer Data, including through the use of:
    - Features that do not enable geo selection such as Content Delivery Network (CDN) that provides a global caching service;
    - Web and Worker Roles, which backup software deployment packages to the United States regardless of deployment geo;
    - Preview, beta, or other pre-release features that may store or transfer Customer Data to the United States regardless of deployment geo;

    - Azure Active Directory (except for Access Control), which may store Active Directory Data globally except for the United States (where Active Directory Data remains in the United States) and Europe (where Active Directory Data is in Europe and the United States);
    - Azure Multi-Factor Authentication, which stores authentication data in the United States;
    - Azure RemoteApp, which may store end user names and device IP addresses globally, depending on where the end user accesses the service.
- Microsoft does not control or limit the geos from which customers or their end users may access Customer Data.

Design and Operational Security

Microsoft has developed industry-leading best practices in the design and management of online services, including:

- **Security Centers of Excellence.** The Microsoft Digital Crimes Unit, Microsoft Cybercrime Center, and Microsoft Malware Protection Center provide insight into evolving global security threats.
- **Security Development Lifecycle (SDL).** Since 2004, all Microsoft products and services have been designed and built from the ground up using its Security Development Lifecycle - a comprehensive approach for writing more secure, reliable and privacy-enhanced code.
- **Operational Security Assurance (OSA).** The Microsoft OSA program provides an operational security baseline across all major cloud services, helping ensure key risks are consistently mitigated.
- **Assume Breach.** Specialized teams of Microsoft security engineers use pioneering security practices and operate with an 'assume breach' mindset to identify potential vulnerabilities and proactively eliminate threats before they become risks to customers.
- **Incident Response.** Microsoft operates a global 24x7 event and incident response team to help mitigate threats from attacks and malicious activity.

Security Controls and Capabilities

Azure delivers a trusted foundation on which customers can design, build and manage their own secure cloud applications and infrastructure.

- **24 hour monitored physical security.** Datacenters are physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as environmental threats.
- **Monitoring and logging.** Security is monitored with the aid of centralized monitoring, correlation, and analysis systems that manage the large amount of information generated by devices within the environment and providing timely alerts. In addition, multiple levels of monitoring, logging, and reporting are available to provide visibility to customers.
- **Patching.** Integrated deployment systems manage the distribution and installation of security patches. Customers can apply similar patch management processes for Virtual Machines deployed in Azure.
- **Antivirus/Antimalware protection.** Microsoft Antimalware is built-in to Cloud Services and can be enabled for Virtual Machines to help identify and remove viruses, spyware and other malicious software and provide real time protection. Customers can also run antimalware solutions from partners on their Virtual Machines.
- **Intrusion detection and DDoS.** Intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools help identify and mitigate threats from both outside and inside of Azure.
- **Zero standing privileges.** Access to customer data by Microsoft operations and support personnel is denied by default. When granted, access is carefully managed and logged. Data center access to the systems that store customer data is strictly controlled via lock box processes.
- **Isolation.** Azure uses network isolation to prevent unwanted communications between deployments, and access controls block unauthorized users. Virtual Machines do not receive inbound traffic from the Internet unless customers configure them to do so.
- **Azure Virtual Networks.** Customers can choose to assign multiple deployments to an isolated Virtual Network and allow those deployments to communicate with each other through private IP addresses.
- **Encrypted communications.** Built-in SSL and TLS cryptography enables customers to encrypt communications within and between deployments, from Azure to on-premises datacenters, and from Azure to administrators and users.

  - **Private connection.** Customers can use ExpressRoute to establish a private connection to Azure datacenters, keeping their traffic off the Internet.

- **Data encryption.** Azure offers a wide range of encryption capabilities up to AES-256, giving customers the flexibility to implement the methods that best meets their needs.
- **Identity and access.** Azure Active Directory enables customers to manage access to Azure, Office 365 and a world of other cloud apps. Multi-Factor Authentication and access monitoring offer enhanced security.

EDUCATION 1DOCSTOP HOSTING ADDENDUM

CA EDUCATION CODE SECTION 490731.1 (AB 1584)

CA BUSINESS & PROFESSIONS CODE SECTION 22584 (SB 1177)

This document shall serve as an addendum to any contract entered into with SyTech Solutions (hereinafter referred to as "Contractor" or "Operator)" and any local educational agency (school district, county office of education, or charter school), hereinafter referred to as "Client" to certify its compliance with California Education Code Section 490731.1 (Assembly Bill 1584) and California Business & Professions Code Section 22584 (Senate Bill 1177).

I. COMPLIANCE WITH CA EDUCATION CODE SECTION 49073.1 (Assembly Bill 1584)

Contractor will fully comply with CA Education Code Section 49073.1 (Assembly Bill 1584).

1.0 DEFINITIONS: For purposes of this section, the following terms have the following meanings pursuant to California Education Code Section 49073.1:

A) "Deidentified information" means information that cannot be used to identify an individual pupil.

B) "Eligible pupil" means a pupil who has reached 18 years of age.

C) "Local educational agency" includes school districts, county offices of education, and charter schools.

D) "Pupil-generated content" means materials created by a pupil, including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, and account information that enables ongoing ownership of pupil content. "Pupil-generated content" does not include pupil responses to a standardized assessment where pupil possession and control would jeopardize the validity and reliability of that assessment.

(1) "Pupil records" means both of the following:

(a) Any information directly related to a pupil that is maintained by the local educational agency.

(b) Any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational agency employee.

(2) "Pupil records" does not mean any of the following:

(a) Deidentified information, including aggregated deidentified information, used by the third party to improve educational products for adaptive learning purposes and for customizing pupil learning.

(b) Deidentified information, including aggregated deidentified information, used to demonstrate the effectiveness of the operator's products in the marketing of those products.

(c) Deidentified information, including aggregated deidentified information, used for the development and improvement of educational sites, services, or applications.

E) "Third party" refers to a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records.

F) "Client" means the local educational agency.

G) "Client Data" includes all Personally Identifiable Information and other information that is not intentionally made generally available by the Client on public websites or publications, including but not limited to business, administrative and financial data, intellectual property, and student and personnel data and metadata.

H) "End User" means the individual(s) authorized by the local educational agency to access and use the Services provided by the Contractor under this Agreement.

I) "Personally Identifiable Information" (or "PII") includes personal identifiers such as name, address, phone number, date of birth, Social Security number, and student or personnel identification number; "pupil records" as defined in California Education Code sections 49060 *et seq*. and/or any successor laws of the California; personally identifiable information contained in student education records as that term is defined in the Family Educational Rights and Privacy Act, 20 USC 1232g; "patient records" as defined in California Health and Safety Code section 123100 *et seq*.; "protected health information" as that term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; nonpublic personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809; credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; other financial account numbers, access codes, driver's license numbers; and state- or federal-identification numbers such as passport, visa or state identity card numbers.

J) "Securely Destroy" means taking actions that render data written on physical (e.g., hardcopy, microfiche, etc.) or electronic media unrecoverable by both ordinary and extraordinary means.

K) "Security Breach" means an event in which Client Data is exposed to unauthorized disclosure, access, alteration, or use.

L) "Services" means any goods or services licensed or provided to the Client from the Contractor, including but not limited to computer software, mobile applications (apps), and web-based tools accessed by students and/or their parents via the Internet and used as part of a school activity, as set forth in the Additional Terms.

M) "Contractor" or "operator" means SyTech Solutions, a C corporation of the State of California having its principal place of business in Elk Grove, California.

N) "Mining Client Data" means to search through, access, or extract Client Data, metadata, or information which is not necessary to accomplish the purpose(s) of this Agreement, to provide the Services, or to improve the Services.

1.1 CONTROL & OWNERSHIP OF STUDENT RECORDS

The Parties agree that as between them, all rights including all intellectual property rights in and to Client Data shall remain the exclusive property of the Client, and Contractor has a limited, nonexclusive license as provided in this Agreement solely for the purpose of performing its obligations hereunder. This Agreement does not give Contractor any rights, implied or otherwise, to Client Data, content, or intellectual property, except as expressly stated in this Agreement.

1.2 STUDENT CONTROL OF CONTENT CREATED FOR SCHOOL

Notwithstanding paragraph (2.1) of this section, the Client's pupils shall retain possession and control of their own pupil-generated content. In order to exert possession and control over their own pupil-generated content, the Client's pupil must provide such requests to the Client in writing. The Client shall pass these requests on to Contractor, and Contractor must reasonably comply, which may include assisting in the facilitation of moving pupil-generated content into a personal account.

1.3 PROHIBITION OF 3RD PARTY USE OF STUDENT INFORMATION FOR PURPOSES OUTSIDE THOSE NAMED IN THIS AGREEMENT

Contractor will use the education records only for the purpose of fulfilling its duties under this Agreement and will not share such data with or disclose it to any third party except as provided for in this Agreement, required by law, or authorized in writing by the Client.

1.4 STUDENT, PARENT & GUARDIAN REVIEW & CORRECT PERSONALLY IDENTIFIABLE INFORMATION

Client pupils, as well as their parents and guardians, shall have the right to review personally identifiable information in a pupil's records retained by Contractor. Client pupils, as well as their parents and guardians, shall also have the right to correct such information if it contains errors. In order to review such information, a request must be submitted to the Client in writing. Client shall pass such requests on to Contractor and Contractor must reasonably comply.

1.5 ACTIONS TAKEN TO ENSURE STUDENT DATA IS SECURE & CONFIDENTIAL

1.5.1: SAS70 CERTIFIED DATA CENTERS

Contractor utilizes Microsoft's SAS70 certified Azure to securely host Client's education records. This solutions is specifically audited for HIPAA and FERPA compliance.

1.5.2: ISO/IEC 27018 & ISO/IEC 27001/27002:2013 CERTIFIED & AUDITED ANNUALLY

Azure is committed to annual certification against ISO/IEC 27001/27002:2013, a broad international information security standard. Additionally, Microsoft Azure services have incorporated the controls that embody ISO/IEC 27018 – an extension of the ISO 27001 standard with a code of practice governing the processing of personal information by cloud service providers. ISO 27018 provides controls that reflect considerations specifically for protecting personally identifiable information in public cloud services. For example, the ISO 27018 controls prohibit the use of customer data for advertising and marketing purposes without the customer's express consent.

1.5.3: SOC 1/SSAE 16/ISAE 3402 and SOC 2 CERTIFIED

Azure has been audited against the Service Organization Control (SOC) reporting framework for both SOC 1 Type 2 and SOC 2 Type 2. Both reports are available to customers to meet a wide range of US and international auditing requirements. The SOC 1 Type 2 audit report attests to the design and operating effectiveness of Azure controls. The SOC 2 Type 2 audit included a further examination of Azure controls related to security, availability, and confidentiality. Azure is audited annually to ensure that security controls are maintained. Audits are conducted in accordance with the Statement on Standards for Attestation Engagements (SSAE) No. 16 put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements (ISAE) 3402 put forth by the International Auditing and Assurance Standards Board (IAASB). In addition, the SOC 2 Type 2 audit included an examination of the Cloud Controls Matrix (CCM) from the Cloud Security Alliance (CSA).

1.5.4: CO-LOCATION & DISASTER RECOVERY

Client Data will not be stored outside the United States. For disaster recovery purposes, hosted Client Data will be securely co-located on at least two separate servers located in the continental United States.

1.5.5: INTRUSION DETECTION & DDoS

Intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools help identify and mitigate threats from both outside and inside of Azure.

1.5.6: 24 HOUR MONITORED PHYSICAL SECURITY

Datacenters are physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as environmental threats.

1.5.7: DATA VERSION BACKUP

Every document stored in 1DocStop is backed up at least once per version using a completely different Azure Service Account. This is done to mitigate any potential threat to top level storage account keys or severe application faults. As each document is saved to 1DocStop, it is queued for backup to the backup service using a first-in first-out serial queue. Because documents are backed up individually, this allows them to be protected earlier and restored faster. Additionally, snapshots are created for existing versions prior to any updates being performed. This ensures that rollbacks can be performed without much fanfare. The restore/revert process can be completed by any authenticated user account with an Administrator Role. These document level backups are kept for the life of the document in geographically redundant locations on the Azure cloud but within the continental US.

1.5.8: TLS TRANSPORT LAYER SECURITY

Built-in SSL and TLS cryptography enables customers to encrypt communications within and between deployments, from Azure to on-premises datacenters, and from Azure to administrators and users.

1.5.9: ACTIVE ACCESS MONITORING & ACCESS LOGS

1DocStop provides reporting capability on not only who has access rights to records, but also reports on who actually logs in, what specific record was accessed, and when the access took place.

1.5.10: OPTIONAL TWO-FACTOR AUTHENTICATION

Mobile phone two-factor authentication allows mobile phones to authenticate themselves, the user uses their personal access license plus a one-time-valid, dynamic passcode consisting of digits that is sent to their mobile device via SMS.

1.5.11: NO ADVERTISING SHARING DATA OR DATA MINING

Contractor's CIO conducts regular training of Contractor's employees to ensure the security and confidentiality of pupil records. Contractor will use Client Data only for the purpose of fulfilling its duties under this Agreement and will not share such data, including anonymized data, with or disclose it to any third party without the prior written consent of the Client, except as required by law and except to third party contractors retained by Contractor to provide services related to the Services under written obligations of confidentiality commensurate with the Contractor's confidentiality obligations to the Client. Contractor will not use Client Data (including metadata) for advertising or marketing purposes.

1.5.12: CONFIDENTIALITY OBLIGATIONS

Contractor will provide access to Client Data to its employees, subcontractors and third party contractors who need to access the data to fulfill Contractor obligations under this Agreement. Contractor will ensure that employees and subcontractors who perform work under this Agreement are bound to strict obligations of confidentiality no less rigorous than those set forth herein. If Contractor will have access to "education records" for the Client's students as defined under the Family Educational Rights and Privacy Act (FERPA), the Contractor acknowledges that for the purposes of this Agreement it will be designated as a "school official" with "legitimate educational interests" in the Client Education records. as those terms have been defined under FERPA and its implementing regulations, and the Contractor agrees to abide by the FERPA limitations and requirements imposed on school officials. Contractor shall train all of its responsible employees on how to comply with those responsibilities imposed by FERPA, through this Agreement, which are applicable to Contractor and its employees. Contractor will use the education records only for the purpose of fulfilling its duties under this Agreement for Client's and its End User's benefit, and will not share such data with or disclose it to any third party except as provided for in this Agreement, required by law, or authorized in writing by the Client.

1.6 PROCEDURES FOR NOTIFYING AFFECTED PARTIES IF THERE IS AN UNAUTHORIZED DISCLOSURE OF STUDENT RECORDS

Upon notification of any potential Security Breaches, Contractor shall promptly investigate and remediate such breaches using industry standard technology. Immediately upon confirming a Security Breach, Contractor will notify the Client, fully investigate the incident, and cooperate fully with the Client's response to the incident. Except as otherwise required by law, Contractor will not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the Client.

1.7 CERTIFICATION THAT STUDENT RECORDS WILL NOT BE RETAINED OR AVAILABLE TO SYTECH ONCE THE CONTRACT IS TERMINATED

Upon termination or expiration of this Agreement, Contractor will return or Securely Destroy Client Data as directed by the Client. Transfer to the Client or a third party designated by the Client shall occur within a reasonable period of time, and without significant interruption in service. In the event that the Client requests destruction of its data, Contractor agrees to Securely Destroy all data in its possession and in the possession of any subcontractors or agents to which the Contractor might have transferred Client data. The Contractor agrees to provide certification of data destruction to the Client upon request. Contractor will notify the Client of impending cessation of its business and any contingency plans, including plans for the transfer and inventory of Client Data.

1.8 COMPLIANCE WITH FAMILY EDUCATIONAL RIGHTS & PRIVACY ACT (FERPA)

(A) Contractor will provide access to Client Data to its employees, subcontractors and third party contractors who need to access the data to fulfill Contractor obligations under this Agreement. Contractor will ensure that employees and subcontractors who perform work under this Agreement are bound to strict obligations of confidentiality no less rigorous than those set forth herein. If Contractor will have access to "education records" for the Client's students as defined under the Family Educational Rights and Privacy Act (FERPA), the Contractor acknowledges that for the purposes of this Agreement it will be designated as a "school official" with "legitimate educational interests" in the Client Education records, as those terms have been defined under FERPA and its implementing regulations, and the Contractor agrees to abide by the FERPA limitations and requirements imposed on school officials. Contractor shall train all of its responsible employees on how to comply with those responsibilities imposed by FERPA, through this Agreement, which are applicable to Contractor and its employees. Contractor will use the education records only for the purpose of fulfilling its duties under this Agreement for Client's and its End User's benefit, and will not share such data with or disclose it to any third party except as provided for in this Agreement, required by law, or authorized in writing by the Client.

(B) Client acknowledges and agrees that SyTech can rely, is relying and will continue to rely on Client's full compliance with the applicable obligations imposed by FERPA, as any such obligations may be amended or modified, with respect to any data that may be accessed, obtained, received, extracted or otherwise used by SyTech (or which may be disclosed in any manner to SyTech by or on behalf of Client), in individualized or aggregate form, in connection with Client's use of the Services and SyTech software.

1.9 PROHIBITION FROM USING PERSONNALY IDENTIFIABLE INFORMATION FROM STUDENT RECORDS TO TARGET ADVERTISING TO STUDENTS

Contractor will not use Client Data or Personally Identifiable Information to engage in targeted advertising.

II. COMPLIANCE WITH CA BUSINESS & PROFESSIONS CODE SECTION 22584 (Senate Bill 1177)

Contractor will fully comply with CA Business and Professions Code Section 22584 (Senate Bill 1177).

(a) For the purposes of this section, "operator" means the operator of an Internet Web site, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes.

(b) Operator shall not knowingly engage in any of the following activities with respect to their site, service, or application:

(1) (A) Engage in targeted advertising on the operator's site, service, or application, or (B) target advertising on any other site, service, or application when the targeting of the advertising is based upon any information, including covered information and persistent unique identifiers, that operator has acquired because of the use of that operator's site, service, or application described in subdivision (a).

(2) Use information, including persistent unique identifiers, created or gathered by the operator's site, service, or application, to amass a profile about a K–12 student except in furtherance of K–12 school purposes.

(3) Sell a student's information, including covered information. This prohibition does not apply to the purchase, merger, or other type of acquisition of an operator by another entity, provided that the operator or successor entity continues to be subject to the provisions of this section with respect to previously acquired student information.

(4) Disclose covered information unless the disclosure is made in

(A) In furtherance of the K–12 purpose of the site, service, or application, provided the recipient of the covered information disclosed pursuant to this subparagraph:

(i) Shall not further disclose the information unless done to allow or improve operability and functionality within that student's classroom or school; and

(ii) Is legally required to comply with subdivision (d);

(B) To ensure legal and regulatory compliance;

(C) To respond to or participate in judicial process;

(D) To protect the safety of users or others or security of the site; or

(E) To a service provider, provided the operator contractually (i) prohibits the service provider from using any covered information for any purpose other than providing the contracted service to, or on behalf of, the operator, (ii) prohibits the service provider from disclosing any covered information provided by the operator with subsequent third parties, and (iii) requires the service provider to implement and maintain reasonable security procedures and practices as provided in subdivision (d).

(c) Nothing in subdivision (b) shall be construed to prohibit the operator's use of information for maintaining, developing, supporting, improving, or diagnosing the operator's site, service, or application.

(d) Operator shall:

(1) Implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information, and protect that information from unauthorized access, destruction, use, modification, or disclosure.

(2) Delete a student's covered information if the school or district requests deletion of data under the control of the school or district.

(e) Notwithstanding paragraph (4) of subdivision (b), operator may disclose covered information of a student, as long as paragraphs (1) to (3), inclusive, of subdivision (b) are not violated, under the following circumstances:

(1) If other provisions of federal or state law require the operator to disclose the information, and the operator complies with the requirements of federal and state law in protecting and disclosing that information.

(2) For legitimate research purposes: (A) as required by state or federal law and subject to the restrictions under applicable state and federal law or (B) as allowed by state or federal law and under the direction of a school, school district, or state department of education, if no covered information is used for any purpose in furtherance of advertising or to amass a profile on the student for purposes other than K–12 school purposes.

(3) To a state or local educational agency, including schools and school districts, for K–12 school purposes, as permitted by state or federal law.

(f) Nothing in this section prohibits an operator from using deidentified student covered information as follows:

(1) Within the operator's site, service, or application or other sites, services, or applications owned by the operator to improve educational products.

(2) To demonstrate the effectiveness of the operator's products or services, including in their marketing.

(g) Nothing in this section prohibits an operator from sharing aggregated deidentified student covered information for the development and improvement of educational sites, services, or applications.

(h) "Online service" includes cloud computing services, which must comply with this section if they otherwise meet the definition of an operator.

(i) "Covered information" means personally identifiable information or materials, in any media or format that meets any of the following:

(1) Is created or provided by a student, or the student's parent or legal guardian, to an operator in the course of the student's, parent's, or legal guardian's use of the operator's site, service, or application for K–12 school purposes.

(2) Is created or provided by an employee or agent of the K–12 school, school district, local education agency, or county office of education, to an operator.

(3) Is gathered by an operator through the operation of a site, service, or application described in subdivision (a) and is descriptive of a student or otherwise identifies a student, including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages,

documents, student identifiers, search activity, photos, voice recordings, or geolocation information.

(j) "K–12 school purposes" means purposes that customarily take place at the direction of the K–12 school, teacher, or school district or aid in the administration of school activities, including, but not limited to, instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents, or are for the use and benefit of the school.

(k) This section shall not be construed to limit the authority of a law enforcement agency to obtain any content or information from an operator as authorized by law or pursuant to an order of a court of competent jurisdiction.

(l) This section does not limit the ability of an operator to use student data, including covered information, for adaptive learning or customized student learning purposes.

(m) This section does not apply to general audience Internet Web sites, general audience online services, general audience online applications, or general audience mobile applications, even if login credentials created for an operator's site, service, or application may be used to access those general audience sites, services, or applications.

(n) This section does not limit Internet service providers from providing Internet connectivity to schools or students and their families.

(o) This section shall not be construed to prohibit an operator of an Internet Web site, online service, online application, or mobile application from marketing educational products directly to parents so long as the marketing did not result from the use of covered information obtained by the operator through the provision of services covered under this section.

(p) This section does not impose a duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance of this section on those applications or software.

(q) This section does not impose a duty upon a provider of an interactive computer service, as defined in Section 230 of Title 47 of the United States Code, to review or enforce compliance with this section by third-party content providers.

(r) This section does not impede the ability of students to download, export, or otherwise save or maintain their own student created data or documents.

Pritt

Signed: ______________________ Date: November 1, 2015

Jon Pritt
Vice President
SyTech Solutions