

STANDARD STUDENT DATA PRIVACY AGREEMENT

**MASSACHUSETTS, MAINE, IOWA, ILLINOIS, MISSOURI, NEW
HAMPSHIRE, NEBRASKA, NEW JERSEY, NEW YORK, OHIO, RHODE
ISLAND, TENNESSEE, VERMONT, AND VIRGINIA**

MA-ME-IA-IL-MO-NH-NE-NJ-NY-OH-RI-TN-VT-VA-NDPA, Standard Version 1.0

St Charles R-VI School District

and

3PI Tech Solutions Inc.

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between: St. Charles R-VI School District, located at 400 N 6th St., Saint Charles, MO 63301 USA (the “**Local Education Agency**” or “**LEA**”) and 3PI Tech Solutions Inc., located at 5600 River Road, Suite 800, Rosemont, IL 60018, USA (the “**Provider**”).

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
 - ☒ If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
 - ☒ If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”).
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: Michailas Ornovskis Title: CISO, DPO

Address: 440 N BARRANCA AVE #9734 COVINA, CA 91723

Phone: +3725017350 Email: michailas@3dprinterros.com

The designated representative for the LEA for this DPA is:

David Taylor, Director of Technology
400 N. 6th Street, Saint Charles, MO 63301
(636) 443-4000 dtaylor@stcharlessd.org


IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

St Charles R-VI School District

By:  Date: Jul 15, 2025
David Taylor (Jul 15, 2025 15:39 CDT)

Printed Name: David Taylor Title/Position: Director of Technology

3PI Tech Solutions Inc

By:  Date: 07/10/2025

Printed Name: Michailas Ornovskis Title/Position: CISO, DPO

STANDARD CLAUSES

Version 3.0

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 including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. 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, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
3. **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 terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data 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 Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data 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 LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the 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.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests.** Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Student Data held by the Provider pursuant to the

Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student 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 acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data:** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit “F”**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit “F”**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
- (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - 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; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
 - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
 - (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
 - (5) In the event of a breach originating from LEA’s use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF 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 **Exhibit "E"** 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. **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. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute 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.
5. **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.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of

all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"

DESCRIPTION OF SERVICES

Dremel DigiLab software

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.	<input checked="" type="checkbox"/>
	Other application technology meta data-Please specify:	<input checked="" type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application	<input checked="" type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/>
	Observation data	<input type="checkbox"/>
	Other assessment data-Please specify:	<input type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>
Communications	Online communications captured (emails, blog entries)	<input type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/>
Demographics	Date of Birth	<input type="checkbox"/>
	Place of Birth	<input type="checkbox"/>
	Gender	<input type="checkbox"/>
	Ethnicity or race	<input type="checkbox"/>
	Language information (native, or primary language spoken by student)	<input type="checkbox"/>
	Other demographic information-Please specify:	<input type="checkbox"/>
Enrollment	Student school enrollment	<input type="checkbox"/>
	Student grade level	<input type="checkbox"/>
	Homeroom	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input type="checkbox"/>
	Year of graduation	<input type="checkbox"/>
	Other enrollment information-Please specify:	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input type="checkbox"/>
	Email	<input type="checkbox"/>
	Phone	<input type="checkbox"/>
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input type="checkbox"/>

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/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	✓
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	✓
	Student app passwords	✓
Student Name	First and/or Last	✓
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.	✓
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	

EXHIBIT “C”

DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student’s identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student’s cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

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 for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an “operator” for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

Student Generated Content: The term “student-generated content” means materials or content created by a student in the services 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 student content.

School Official: For the purposes of this DPA and pursuant to 34 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 Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

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, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or 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, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** 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.

Subprocessor: For the purposes of this DPA, 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 service, and who has access to Student Data.

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

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

[Insert Name of District or LEA] Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

_____ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

_____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

_____ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By **[Insert Date]**

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

EXHIBIT “F”
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
<input type="checkbox"/>	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
<input checked="" type="checkbox"/>	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input type="checkbox"/>	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
<input type="checkbox"/>	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G"
Massachusetts

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Massachusetts;

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Massachusetts does not require data to be stored within the United States.

EXHIBIT "G"
Maine

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Maine. Specifically, those laws are 20-A M.R.S. §6001-6005.; 20-A M.R.S. §951 et. seq., Maine Unified Special Education Regulations, Maine Dep't of Edu. Rule Ch. 101; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Maine;

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
4. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
5. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
6. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
7. The parties agree that the definition of Student Data in Exhibit "C" includes information that:
 - a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;
 - b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or
 - c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes.

EXHIBIT “G”

Illinois

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Illinois. Specifically, those laws are to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/, and Local Records Act (“LRA”), 50 ILCS 205; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Illinois;

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

1. Paragraph 4 on page 2 of the DPA setting a three-year term for the DPA shall be replaced with: “This DPA shall be effective upon the date of signature by Provider and LEA, and shall remain in effect as between Provider and LEA 1) for so long as the Services are being provided to the LEA or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first. The Exhibit E General Offer will expire three (3) years from the date the original DPA was signed.”
2. Replace Notices with: “Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or four (4) days after mailing, if by first-class mail, postage prepaid.”
3. In Article II, Section 1, add: “Further clarifying, in accordance with FERPA, ISSRA and SOPPA, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; is under the direct control of the LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose and in furtherance of such legitimate educational interest.”
4. In Article II, Section 2, replace “forty five (45)” with “five (5)”. Add the following sentence: “In the event that the LEA determines that the Provider is maintaining Student Data that contains a factual inaccuracy, and Provider cooperation is required in order to make a correction, the LEA shall notify the Provider of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, the Provider shall correct the

factual inaccuracy and shall provide written confirmation of the correction to the LEA.”

5. In Article II, Section 4, replace it with the following: “In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure.”
6. In Article II, Section 5, add: “By no later than (5) business days after the date of execution of the DPA, the Provider shall provide the LEA with a list of any subcontractors to whom Student Data may be disclosed or a link to a page on the Provider's website that clearly lists any and all subcontractors to whom Student Data may be disclosed. This list shall, at a minimum, be updated and provided to the LEA by the beginning of each fiscal year (July 1) and at the beginning of each calendar year (January 1).”
7. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
8. In Article IV, Section 6, replace the whole section with:

The Provider shall review, on an annual basis, whether the Student Data it has received pursuant to the DPA continues to be needed for the purpose(s) of the Service Agreement and this DPA. If any of the Student Data is no longer needed for purposes of the Service Agreement and this DPA, the Provider will provide written notice to the LEA as to what Student Data is no longer needed. The Provider will delete or transfer Student Data in readable form to the LEA, as directed by the LEA (which may be effectuated through Exhibit D of the DPA), within 30 calendar days if the LEA requests deletion or transfer of the Student Data and shall provide written confirmation to the LEA of such deletion or transfer. Upon termination of the Service Agreement between the Provider and LEA, Provider shall conduct a final review of Student Data within 60 calendar days.

If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving the request.

Any provision of Student Data to the LEA from the Provider shall be transmitted in a format readable by the LEA.

9. All employees of the Provider who will have direct contact with students shall pass criminal background checks.

10. In Article IV, Section 7, add “renting,” after “using.”
11. In Article V, Section 1 Data Storage: Illinois requires all Student Data to be stored within the United States, Canada, United Kingdom and/or the European Union.
12. In Article V, Section 4, add the following: “‘Security Breach’ does not include the good faith acquisition of Student Data by an employee or agent of the Provider or LEA for a legitimate educational or administrative purpose of the Provider or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure.”
13. In Article V, Section 4(1) add the following:
 - vi. A list of the students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known; and
 - vii. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.
14. In Article V, Section 4, add a section (6) which states:

In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, without regard to any limitation of liability provision otherwise agreed to between Provider and LEA, including but not limited to costs and expenses associated with:

 - a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;
 - b. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the student's credit or financial security;
 - c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA as a result of the security breach; and
 - d. Providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws.
15. Replace Article VII, Section 1 with: “In the event either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or been terminated. One party may terminate this DPA upon a material breach of this DPA by the other party. Upon termination of the DPA, the Service Agreement shall terminate.”

16. In Exhibit C, add to the definition of Student Data, the following: “Student Data includes any and all information concerning a student by which a student may be individually identified under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school student records", “student temporary record” or “student permanent record” as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)) (c) “records” as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) “personal information” as defined in Section 530/5 of PIPA.”
17. The following shall be inserted as a new second sentence in Paragraph 1 of Exhibit E: “The provisions of the original DPA offered by Provider and accepted by Subscribing LEA pursuant to this Exhibit E shall remain in effect as between Provider and Subscribing LEA 1) for so long as the Services are being provided to Subscribing LEA, or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first.”
18. The Provider must publicly disclose material information about its collection, use, and disclosure of Student Data, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.
19. **Minimum Data Necessary Shared.** The Provider attests that the Student Data request by the Provider from the LEA in order for the LEA to access the Provider’s products and/or services is limited to the Student Data that is adequate, relevant, and limited to what is necessary in relation to the K-12 school purposes for which it is processed.
20. **Student and Parent Access.** Access by students or parents/guardians to the Provider’s programs or services governed by the DPA or to any Student Data stored by Provider shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this DPA.
21. **Exhibits A and B.** The Services described in Exhibit A and the Schedule of Data in Exhibit B to the DPA satisfy the requirements in SOPPA to include a statement of the product or service being provided to the school by the Provider and a listing of the categories or types of covered information to be provided to the Provider, respectively.
22. The Provider will not collect social security numbers.

EXHIBIT “G”

Iowa

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Iowa. Specifically, those laws are Iowa Code §§ 22; Iowa Code §§ 715C, 281 I.A.C. 12.3(4); 41; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Iowa;

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

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Iowa does not require all Student Data to be stored within the United States.
4. In Exhibit “C” add to the definition of “Student Data” significant information on progress and growth, experiences, interests, aptitudes, attitudes, abilities, part-time employment, and future plans.

EXHIBIT “G”

Missouri

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Missouri. Specifically, those laws are Sections 162.1475 and 407.1500 RSMo; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Missouri;

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

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Missouri does not require data to be stored within the United States.
4. Replace Article V, Section 4(1) with the following:
 - a. In the event of a breach of data maintained in an electronic form that includes personal information of a student or a student’s family member, Provider shall notify LEA within seventy-two (72) hours. The notice shall include:
 - i. Details of the incident, including when it occurred and when it was discovered;
 - ii. The type of personal information that was obtained as a result of the breach; and
 - iii. The contact person for Provider who has more information about the incident.
 - b. “*Breach*” shall mean the unauthorized access to or unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person employed by or contracted with, or an agent of, Provider is not a breach provided that the personal information is not used in violation of applicable Federal or Missouri law, or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.
 - c. “*Personal information*” is the first name or initial and last name of a student or a family member of a student in combination with any one or more of the following data items that relate to the student or a family member of the student if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology such that the name or data elements are unreadable or unusable:
 - i. Social Security Number;
 - ii. Driver’s license number or other unique identification number created or collected by a government body;
 - iii. Financial account information, 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;
 - iv. Unique electronic identifier or routing code in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
 - v. Medical information; or
 - vi. Health insurance information.

EXHIBIT "G"
Nebraska

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Nebraska. Specifically, those laws are Neb. Rev. Stat. Secs. 79-2,104; 79-2,153 to 79-2,155; 79-2, 539; 87-801 to 87-808; and 92 NAC 6; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Nebraska;

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

1. In Article II, Section 5, add, "Specifically, any written agreement with a Subprocessor will: (1) prohibit the Subprocessor from using Student Data any purpose other than providing the contracted service to or on behalf of the Provider; (2) prohibit the Subprocessor from disclosing any Student Data provided by the Provider with subsequent third parties; (3) and requires the Subprocessor to implement and maintain reasonable security procedures and practices."
2. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
3. In Article IV, Section 4, replace: "Provider will not Sell Student Data to any third party" with "Provider will not Sell or rent Student Data to any third party."
4. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
5. In Article V, Section 1 Data Storage: Nebraska does not require data to be stored within the United States.

EXHIBIT "G"
New Jersey

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Jersey. Specifically, those laws are N.J. Stat. § 56:8-166.4 et seq.; N.J. Stat. § 18A:36-19; N.J. Stat. § 18A:36-19a; N.J. Stat. § 18A:36-35; N.J. Admin Code § 6A:16-7.9; N.J. Admin. Code § 6A:32-2.1; N.J. Admin. Code § 6A:32-7 et. seq.; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Jersey;

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. The Provider will not disclose on its web site any personally identifiable information about a student, including, but not limited to student names, student photos, student addresses, student e-mail addresses, student phone numbers, and locations and times of class trips.
4. The Provider will not process Student Data in violation of State and federal laws that prohibit unlawful discrimination.
5. The Provider will not conduct processing that presents a heightened risk of harm to students without conducting and documenting a data protection assessment of each of its processing activities that involve Student Data.
6. In Article V, Section 1 Data Storage: New Jersey does not require data to be stored within the United States.
7. Add to the definition in Exhibit "C" of Student Data: "The location and times of class trips."

EXHIBIT "G"

Ohio

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Ohio. Specifically, those laws are R.C. §§ 3319.32-3319.327, R.C. §§ 1349.17-19, Rule 3301-51-04; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Ohio;

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. In Article IV, Section 3, add: "The Provider will restrict unauthorized access by Provider's employees or contractors not providing services under the Service Agreement or DPA and its employees or contractors will only access Student Data as necessary to fulfill their official duties."
3. In Article IV, Section 6, replace "Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice," with "Upon termination of this DPA, unless the LEA provides notice that renewal of the contract is reasonably anticipated, within ninety (90) days of the expiration of the contract, Provider shall destroy or return Student Data to the LEA."
4. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
5. In Article V, Section 1 Data Storage: Ohio does not require data to be stored within the United States.
6. Provider will not access or monitor any of the following:
 - a. Location-tracking features of a school-issued device;
 - b. Audio or visual receiving, transmitting or recording features of a school-issued device;
 - c. Student interactions with a school-issued device, including, but not limited to, keystrokes and web-browsing activity

Notwithstanding the above, if the Provider has provided written notice to the LEA that it engages in this collection of the above information, which must be provided in the Service Agreement, and the LEA has provided written confirmation that the Provider can collect this information pursuant to its general monitoring, then the Provider may access or monitor the listed information.

EXHIBIT "G"
Rhode Island

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Rhode Island. Specifically, those laws are R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16- 104-1, and R.I.G.L., 11-49.3 et. seq.; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Rhode Island;

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
4. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
5. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
6. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
 - i. Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact:
 1. The credit reporting agencies
 2. Remediation service providers
 3. The attorney general
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
 - iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student's requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

EXHIBIT “G”
Tennessee

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Tennessee. Specifically, those laws are T.C.A. §§ 10-7-503 *et. seq.*, T.C.A. § 47-18-2107, T.C.A. § 49-1-701 *et. seq.*, T.C.A. § 49-2-211, T.C.A. § 49-6-902, § 49-6-3001, T.C.A. §§ 49-50-1501 *et. seq.*; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Tennessee;

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

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Tennessee does not require data to be stored within the United States.
4. The Provider agrees that it will not collect any individual student biometric data, student data relative to analysis of facial expressions, EEG brain wave patterns, skin conductance, galvanic skin response, heart-rate variability, pulse, blood volume, posture, and eye-tracking.
5. The Provider agrees that it will not collect individual student data on:
 - a. Political affiliation;
 - b. Religion;
 - c. Voting history; and
 - d. Firearms ownership

EXHIBIT “G”

Vermont

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Vermont. Specifically, those laws are 9 VSA 2443 to 2443f; 16 VSA 1321 to 1324; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Vermont;

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

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

EXHIBIT “G”
Virginia

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Virginia. Specifically, those laws are Code of Virginia § 22.1-289.01 and Virginia Code § 2.2-5514(c); and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Virginia;

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

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Virginia does not require data to be stored within the United States.
4. In Article V, Section 4, add: In order to ensure the LEA’s ability to comply with its reporting requirements under Virginia Code § 2.2-5514(c), Provider shall provide initial notification to the LEA as soon as reasonably practical, and at a minimum within twenty-four (24) hours, where the Provider reasonably expects or confirms Student Data may have been disclosed in a data breach.

EXHIBIT "G"
New Hampshire

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Hampshire;

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

1. All references in the DPA to "Student Data" shall be amended to state "Student Data and Teacher Data." "Teacher Data" is defined as at least the following:

Social security number.

Date of birth.

Personal street address.

Personal email address.

Personal telephone number

Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

"Teacher" means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "I"**.
3. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
4. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,..."
5. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
6. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as

necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes.

7. The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:
 - (1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
 - (2) Limit unsuccessful logon attempts;
 - (3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
 - (4) Authorize wireless access prior to allowing such connections;
 - (5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
 - (6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;
 - (7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
 - (8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;
 - (9) Enforce a minimum password complexity and change of characters when new passwords are created;
 - (10) Perform maintenance on organizational systems;
 - (11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
 - (12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;
 - (13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;
 - (14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
 - (15) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;
 - (16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

- (17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;
- (18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);
- (19) Protect the confidentiality of Student Data and Teacher Data at rest;
- (20) Identify, report, and correct system flaws in a timely manner;
- (21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;
- (22) Monitor system security alerts and advisories and take action in response; and
- (23) Update malicious code protection mechanisms when new releases are available.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

- 8. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
 - i. The estimated number of students and teachers affected by the breach, if any.
- 9. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.
- 10. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.

EXHIBIT "I" – TEACHER 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	✓
Communications	Online communications that are captured (emails, blog entries)	
Demographics	Date of Birth	
	Place of Birth	
	Social Security Number	
	Ethnicity or race	
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	
	Personal Email	
	Personal Phone	
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	
	Teacher calendar	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Teacher app username	✓
	Teacher app passwords	✓
Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
Teacher work	Teacher generated content; writing, pictures etc.	
	Other teacher work data -Please specify:	
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

Exhibit “G”

New York

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the DPA.
3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA's Data Security and Privacy Policy. The LEA's Data Security Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security Policy to the Provider upon execution of Exhibit “E”. Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations.
4. Provider represents that their Data Privacy and Security Plan can be found at the URL link listed in Exhibit K and is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a) implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the service agreement; (c) complies with the LEA's parents bill of rights for data privacy and security; (d) requires training of all providers' employees, assignees and subprocessors who have Access to student data or APPR data; (e) ensures subprocessors are required to protect PII received under this service agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, deletion and destruction.
5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit “E”.
6. All references in the DPA to “Student Data” shall be amended to include and state, “Student Data and APPR Data.”
7. To amend Article II, Section 5 to add: Provider shall ensure that its subprocessors agree that they do not have any property, licensing or ownership rights or claims to Student Data or APPR data and that they will comply with the LEA's Data Privacy and Security Policy. Provider shall examine the data privacy and security measures of its Subprocessors. If at any point a Subprocessor fails to materially comply with the requirements of this DPA, Provider shall: (i) notify LEA, (ii) as applicable, remove such Subprocessor's Access to Student Data and APPR Data; and (iii) as applicable, retrieve all Student Data and APPR Data received or stored by such

Subprocessor and/or ensure that Student Data and APPR Data has been securely deleted or securely destroyed in accordance with this DPA. In the event there is an incident in which Student Data and APPR Data held, possessed, or stored by the Subprocessor is compromised, or unlawfully Accessed or disclosed, Provider shall follow the Data Breach reporting requirements set forth in the DPA.

8. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
9. To amend Article IV, Section 3 to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data and APPR Data will be trained on the federal and state laws governing confidentiality of such Student Data and APPR Data prior to receipt. Access to or Disclosure of Student Data and APPR Data shall only be provided to Provider’s employees and subprocessors who need to know the Student Data and APPR Data to provide the services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide such services.
10. To replace Article IV, Section 6 (Disposition of Data) with the following: Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider’s certifying that it and it’s subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any assurance of discontinuation, which will control in the case of a conflict.

Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all student data after providing the LEA with ninety (90) days prior notice.

The duty to dispose of student data shall not extend to Student Data that had been de-identified or placed in a separate student account pursuant to section II 3. The LEA may employ a “**Directive for Disposition of Data**” form, a copy of which is attached hereto as **Exhibit “D”**, or, with reasonable notice to the Provider, other form of its choosing. No further written request or notice is required on the part of either party prior to the disposition of Student Data described in “**Exhibit D**”.

11. To amend Article IV, Section 7 to add: 'Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, "which term shall not include students."
12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
13. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an unauthorized Access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA or its designee(s) to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA or its designee(s) and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable Access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.

Upon request by the New York State Education Department's Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require Provider to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider's expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider's privacy and security practices that was issued no more than twelve months before the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the NIST Cybersecurity Framework v1.1 or any update to this Framework that is adopted by the New York State Department of Education.

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt

investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

- (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - 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; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and
 - vi. The number of records affected, if known; and
 - vii. A description of the investigation undertaken so far; and
 - viii. The name of a point of contact for Provider.
- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.
- (6) Provider and its subprocessors will cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

15. To amend the definitions in Exhibit "C" as follows:

- “Subprocessor” is equivalent to subcontractor. It is a third party who the provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its service, and who has access to Student Data.
- “Provider” is also known as third party contractor. It any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

16. To add to Exhibit “C” the following definitions:

- **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting.
- **APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d
- **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration, including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.
- **Disclose or Disclosure:** The intentional or unintentional communication, release, or transfer of Student Data and/or APPR Data by any means, including oral, written, or electronic.
- **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
- **Release:** Shall have the same meaning as Disclose
- **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services, then the term LEA shall also include Participating School

Districts for purposes of the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.

- **Participating School District:** As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement with LEA, and shall include LEA if it uses the Services in its own educational or operational programs.

-

Exhibit “J”
LEA Documents

New York LEAs will provide links to their Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy, and supplemental information for this service agreement in their Exhibits.

Exhibit “K”
Provider Security Policy

Provider’s Data Security and Privacy Plan can be accessed at:
System Security Plan document (TX-RAMP) is sent via email as an attachment



STATERAMP SYSTEM SECURITY PLAN (SSP)

3D CONTROL SYSTEMS
3DPRINTEROS

VERSION:

1.1


DATE:

20250130




SYSTEM SECURITY PLAN

Prepared by:

Identification of Organization that Prepared this Document		
	Organization Name	3D Control Systems
	Street Address	340 South Lemon Avenue
	Suite/Room/Building	Suite 9734
	City, State Zip	Walnut, CA 91789

Prepared for:

Identification of Cloud Service Provider		
	Organization Name	3D Control Systems
	Street Address	340 South Lemon Avenue
	Suite/Room/Building	Suite 9734
	City, State Zip	Walnut, CA 91789

TEMPLATE REVISION HISTORY

Date	Description
3/31/2021	Original publication



DOCUMENT REVISION HISTORY

Date	Description	Version of SSP	Author
6/2/2024	Initial revision for given template version	1.0	Michailas Ornovskis, CISO
1/30/2025	Reviewed to version 1.1	1.1	Michailas Ornovskis, CISO
<Date>	<Revision Description>	<Version>	<Author>



TABLE OF CONTENTS

1. INFORMATION SYSTEM NAME/TITLE	1
2. INFORMATION SYSTEM CATEGORIZATION	1
2.1 INFORMATION TYPES	1
2.1.1 CATEGORY 1.....	1
2.1.2 CATEGORY 3.....	1
2.2 SECURITY OBJECTIVES CATEGORIZATION	2
2.3 DIGITAL IDENTITY DETERMINATION	2
3. INFORMATION SYSTEM OWNER	3
4. AUTHORIZING OFFICIAL.....	3
5. OTHER DESIGNATED CONTACTS.....	3
6. ASSIGNMENT OF SECURITY RESPONSIBILITY.....	5
7. INFORMATION SYSTEM OPERATIONAL STATUS.....	6
8. INFORMATION SYSTEM TYPE.....	6
8.1 CLOUD SERVICE MODELS	6
8.2 CLOUD DEPLOYMENT MODELS	7
8.3 LEVERAGED AUTHORIZATIONS	7
9. GENERAL SYSTEM DESCRIPTION	8
9.1 SYSTEM FUNCTION OR PURPOSE	8
9.2 INFORMATION SYSTEM COMPONENTS AND BOUNDARIES	8
9.3 TYPES OF USERS	9
9.4 NETWORK ARCHITECTURE	11
9.5 DATA FLOW	13
9.6 PORTS, PROTOCOLS AND SERVICES.....	15
10. SYSTEM INTERCONNECTIONS.....	16
11. MINIMUM SECURITY CONTROLS.....	17
12. SYSTEM SECURITY PLAN ATTACHMENTS	24
13. DIGITAL IDENTITY WORKSHEET.....	26
13.1 INTRODUCTION AND PURPOSE	26
13.2 INFORMATION SYSTEM NAME/TITLE	26
13.3 DIGITAL IDENTITY LEVEL DEFINITIONS	26
13.4 REVIEW MAXIMUM POTENTIAL IMPACT LEVELS.....	27
13.5 DIGITAL IDENTITY LEVEL SELECTION	28
14. PTA AND PIA	29
14.1 PRIVACY OVERVIEW AND POINT OF CONTACT (POC)	29
14.2 PERSONALLY IDENTIFIABLE INFORMATION (PII)	30
14.3 PRIVACY DESIGNATION.....	30



14.4 THRESHOLD ANALYSIS	30
14.5 PRIVACY IMPACT ASSESSMENT TALKING POINTS.....	30
14.6 PII MAPPING OF COMPONENTS (SE-1, DM-1)	31
14.7 PROSPECTIVE PII USE	32
14.8 SOURCES OF PII AND PURPOSE	32
14.9 ACCESS TO PII AND SHARING	32
14.10 PII SAFEGUARDS AND LIABILITIES.....	33
14.11 CONTRACTS, AGREEMENTS, AND OWNERSHIP	34
14.12 ACCURACY OF THE PII AND REDRESS	34
14.13 MAINTENANCE AND ADMINISTRATIVE CONTROLS	34
14.14 BUSINESS PROCESSES AND TECHNOLOGY.....	35
14.15 PRIVACY POLICY	35
14.16 SIGNATURES.....	36
15. SECURITY CATEGORIZATION	37
15.1 INSTRUCTIONS	37
15.2 SURVEY QUESTIONS	37



LIST OF FIGURES

Figure 9-2 Network Diagram.....	12
Figure 10-1 Data Flow Diagram	15


LIST OF TABLES

Table 1. Information System Name and Title	1
Table 2. Security Categorization	1
Table 3. Security Impact Level	2
Table 4. Baseline Security Configuration	2
Table 5. Information System Owner	3
Table 6. Information System Management Point of Contact	3
Table 7. Information System Technical Point of Contact.....	3
Table 8. CSP Name Internal ISSO (or Equivalent) Point of Contact	5
Table 9. AO Point of Contact.....	5
Table 10. System Status	6
Table 11. Service Layers Represented in this SSP	7
Table 12. Cloud Deployment Model Represented in this SSP	7
Table 13. Leveraged Authorizations	8
Table 14. Personnel Roles and Privileges.....	10
Table 15 Ports, Protocols, and Services	15
Table 16. System Interconnections.....	16
Table 17. Summary of Required Security Controls	17
Table 18. Control Origination and Definitions	23
Table 19. Names of Provided Attachments	24
Table 20. Information System Name and Title	26
Table 21. Mapping StateRAMP Levels to NIST SP 800-63-3 Levels.....	27
Table 22. Potential Impacts for Assurance Levels	27
Table 23. Digital Identity Level.....	28
Table 24. Information System Name; Privacy POC	29
Table 25 PII Mapped to Components	31



SYSTEM SECURITY PLAN APPROVALS

Cloud Service Provider Signatures

			
Name	Michailas Ornovskis	Date	6/2/2024
Title	Chief Information Security Officer		
Cloud Service Provider	3DPrinterOS (product of 3D Control Systems), also known as 3D Control Systems: 3DPrinterOS		



1. INFORMATION SYSTEM NAME/TITLE

This System Security Plan provides an overview of the security requirements for the Information System Name 3DPrinterOS and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed, or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed, or stored by the 3DPrinterOS information system.

The security safeguards implemented for the 3DPrinterOS system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures, and practices.

Table 1. Information System Name and Title

Unique Identifier	Information System Name	Information System
TX-RAMP, Cert ID TX1071880	3DPrinterOS	3DPrinterOS

2. INFORMATION SYSTEM CATEGORIZATION

The overall information system sensitivity categorization is recorded in Table 2. Security Categorization that follows.

Table 2. Security Categorization

System Sensitivity Level:	Category 1
---------------------------	------------

2.1 INFORMATION TYPES

2.1.1 CATEGORY 1

The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

2.1.2 CATEGORY 3

The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for



example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

2.2 SECURITY OBJECTIVES CATEGORIZATION

For the 3DPrinterOS, default to the high-water mark for the Information Types as identified in Table 3. Security Impact Level below.

Table 3. Security Impact Level

Security Objective	Low, Moderate, or High
	Low (L)
	Low (L)
	Low (L)

Through review and analysis, it has been determined that the baseline security categorization for the Enter Information System Abbreviation system is listed in the Table 4. Baseline Security Configuration that follows.

Table 4. Baseline Security Configuration

Enter Information System Abbreviation Security	Category 1
--	------------

Using this categorization, in conjunction with the risk assessment and any unique security requirements, we have established the security controls for this system, as detailed in this SSP.

2.3 DIGITAL IDENTITY DETERMINATION

The digital identity information may be found in **Error! Reference source not found.**

Note: NIST SP 800-63-3, Digital Identity Guidelines, does not recognize the four Levels of Assurance model previously used by federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels corresponding to each function being performed. The digital identity level is Level 1: AAL1, IAL1, FAL1



3. INFORMATION SYSTEM OWNER

The following individual is identified as the system owner or functional proponent/advocate for this system.

Table 5. Information System Owner

Information System Owner Information	
Name	Artem Lozinsky
Title	Product Owner, Information System Owner and Manager
Company / Organization	3D Control Systems
Address	340 S Lemon Ave #9734, Walnut, CA 91789, USA
Phone Number	+380673241571
Email Address	artem.lozinsky@3dprinteros.com

4. AUTHORIZING OFFICIAL

The Authorizing Official (AO) for this information system is the Texas DIR (for TX-RAMP).

5. OTHER DESIGNATED CONTACTS

The following individual(s) identified below possess in-depth knowledge of this system and/or its functions and operation.

Table 6. Information System Management Point of Contact

Information System Management Point of Contact	
Name	Artem Lozinsky
Title	Product Owner, Information System Owner and Manager
Company / Organization	3D Control Systems
Address	340 S Lemon Ave #9734, Walnut, CA 91789, USA
Phone Number	+380673241571
Email Address	artem.lozinsky@3dprinteros.com

Table 7. Information System Technical Point of Contact

Information System Technical Point of Contact	
Name	Maksym Kozlov
Title	System Administrator
Company / Organization	3D Control Systems
Address	340 S Lemon Ave #9734, Walnut, CA 91789, USA



Information System Technical Point of Contact	
Phone Number	+380504060873
Email Address	m.kozlov@3dprinterOS.com



6. ASSIGNMENT OF SECURITY RESPONSIBILITY

The Information System Security Officers (ISSO), or their equivalent, identified below, have been appointed in writing and are deemed to have significant cyber and operational role responsibilities.

Table 8. CSP Name Internal ISSO (or Equivalent) Point of Contact

CSP Name Internal ISSO (or Equivalent) Point of Contact	
Name	Michailas Ornovskis
Title	Chief Information Security Officer
Company / Organization	3D Control Systems
Address	340 S Lemon Ave #9734, Walnut, CA 91789, USA
Phone Number	+3725017350
Email Address	michailas@3dprinterOS.com

Table 9. AO Point of Contact

AO Point of Contact	
Name	Texas DIR
Title	-
Organization	Texas DIR
Address	300 W. 15th Street, Suite 1300, Austin, TX 78701
Phone Number	512-475-4700
Email Address	dir@dir.texas.gov



7. INFORMATION SYSTEM OPERATIONAL STATUS

The system is currently in the lifecycle phase shown in Table 10. System Status that follows. (Only operational systems can be granted an ATO).

Table 10. System Status

System Status		
<input checked="" type="checkbox"/>	Operational	The system is operating and in production.
<input type="checkbox"/>	Under Development	The system is being designed, developed, or implemented
<input type="checkbox"/>	Major Modification	The system is undergoing a major change, development, or transition.
<input type="checkbox"/>	Other	Explain: Click here to enter text.

8. INFORMATION SYSTEM TYPE

The 3DPrinterOS makes use of unique managed service provider architecture layer(s). System architecture is split into three-tier model, all components reside in Microsoft Azure Cloud.

8.1 CLOUD SERVICE MODELS

Information systems, particularly those based on cloud architecture models, are made up of different service layers. Below are some questions that help the system owner determine if their system is a cloud followed by specific questions to help the system owner determine the type of cloud.

Question (Yes/No)	Conclusion
Does the system use virtual machines?	Yes.
Does the system have the ability to expand its capacity to meet customer demand?	Yes.
Does the system allow the consumer to build anything other than servers?	Yes.
Does the system offer the ability to create databases?	No.
Does the system offer various developer toolkits and APIs?	Yes.
Does the system offer only applications that are available by obtaining a login?	Yes.

The layers of the 3DPrinterOS defined in this SSP are indicated in Table 11. Service Layers Represented in this SSP that follows.



Table 11. Service Layers Represented in this SSP

Service Provider Architecture Layers		
<input checked="" type="checkbox"/>	Software as a Service (SaaS)	Major Application
<input type="checkbox"/>	Platform as a Service (PaaS)	Major Application
<input type="checkbox"/>	Infrastructure as a Service (IaaS)	General Support System
<input type="checkbox"/>	Other	Explain: Click here to enter text.

Note: Refer to NIST SP 800-145 for information on cloud computing architecture models.

8.2 CLOUD DEPLOYMENT MODELS

Information systems are made up of different deployment models. The deployment models of the 3DPrinterOS that are defined in this SSP and are not leveraged by any other StateRAMP or TX-RAMP Authorizations, are indicated in Table 12. Cloud Deployment Model Represented in this SSP that follows.

Table 12. Cloud Deployment Model Represented in this SSP

Service Provider Cloud Deployment Model		
<input checked="" type="checkbox"/>	Public	Cloud services and infrastructure supporting multiple organizations and agency clients
<input type="checkbox"/>	Private	Cloud services and infrastructure dedicated to a specific organization/agency and no other clients
<input type="checkbox"/>	Government Only Community	Cloud services and infrastructure shared by several organizations/agencies with same policy and compliance considerations
<input type="checkbox"/>	Hybrid	Explain: (e.g., cloud services and infrastructure that provides private cloud for secured applications and data where required and public cloud for other applications and data) Click here to enter text.

8.3 LEVERAGED AUTHORIZATIONS

The 3DPrinterOS plans to leverage a pre-existing StateRAMP or TX-RAMP Authorization. StateRAMP and/or TX-RAMP Authorizations leveraged by this 3DPrinterOS are listed in Table 13. Leveraged Authorizations that follows.



Table 13. Leveraged Authorizations

Leveraged Information System Name	Leveraged Service Provider Owner	Date Granted
3DPrinterOS	3D Control Systems	2/14/2023
<Enter Leveraged information system name2>	<Enter service provider owner2>	None
<Enter Leveraged information system name3>	<Enter service provider owner3>	None

9. GENERAL SYSTEM DESCRIPTION

This section includes a general description of the Enter Information System Abbreviation.

9.1 SYSTEM FUNCTION OR PURPOSE

3DPrinterOS is a 3D Printing cloud-based solution, mainly for Educational Institutions. 3DPrinterOS allows to manage all of organization 3D printers and users in a single platform.

3DPrinterOS makes it simple for users of any skill-level to start and keep printing successfully. Visualize, repair, prepare and slice models for 3D printing with only a few clicks.

3DPrinterOS has the highest security levels for end-to-end encrypted 3D printing workflows in the industry.

9.2 INFORMATION SYSTEM COMPONENTS AND BOUNDARIES

A detailed and explicit definition of the system authorization boundary diagram is represented in Figure 9-2 Authorization Boundary Diagram below.

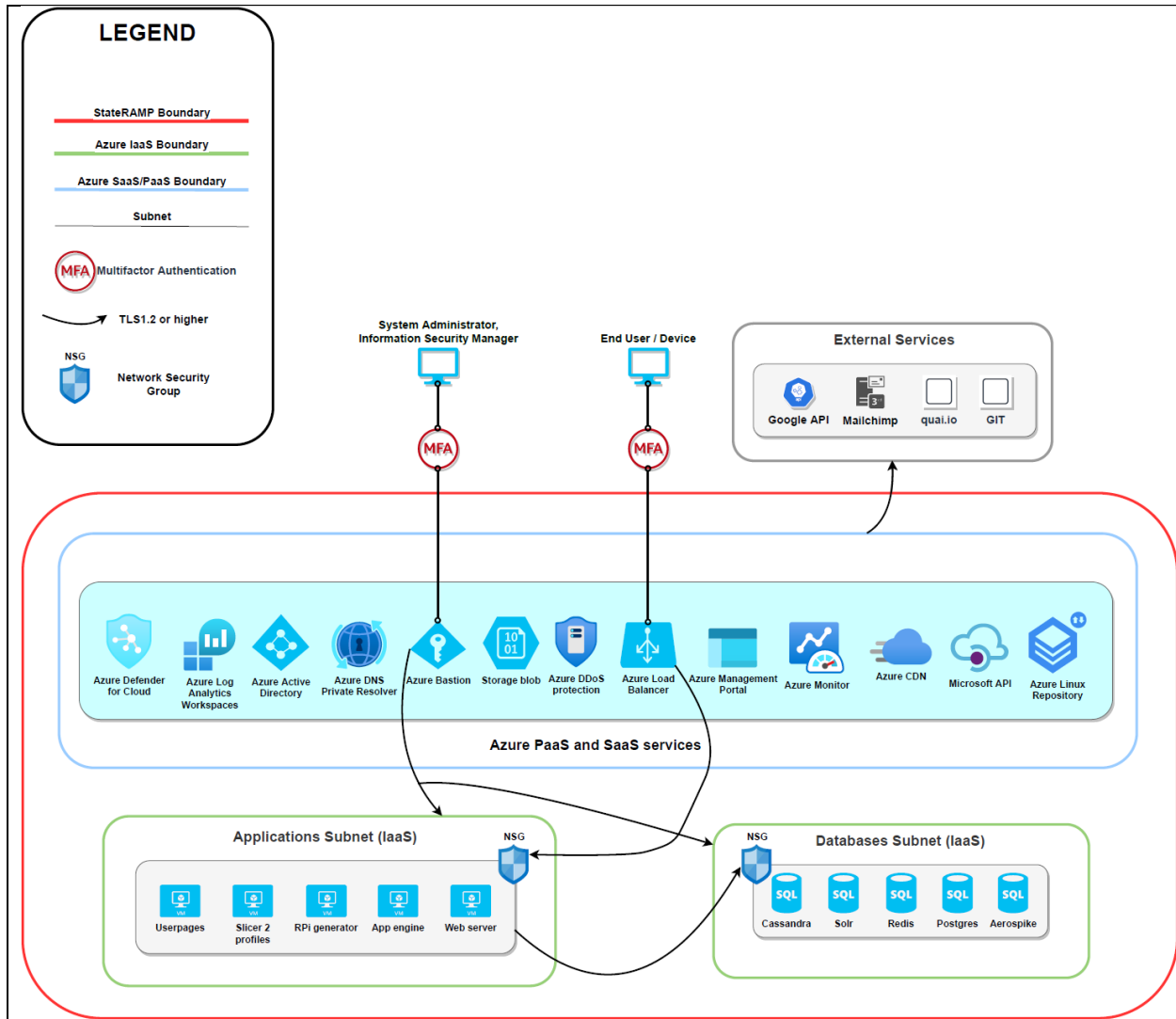


Figure 9-2 Authorization Boundary Diagram

9.3 TYPES OF USERS

All personnel have their status categorized with a sensitivity level in accordance with PS-2. Personnel (employees or contractors) of service providers are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in Table 14. Personnel Roles and Privileges that follows.



Table 14. Personnel Roles and Privileges

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed
System Administrator	Internal	P	Moderate	Full administrative access to backend (root)	Install and manage virtual machines, cloud configuration settings, install, and configure software, OS updates, patches, and hotfixes, perform backups.
Database Administrator	Internal	P	Moderate	Databases administrative access	Install and manage databases, configure database servers' settings, apply hotfixes and perform backups.
User Account Administrator	Internal	NP	Limited	User Account Management, IAM	Add, remove and manage user accounts in administrative cloud (Azure).
Security Administrator	Internal	NP	Limited	Manage cloud security configuration settings	Manage cloud security configuration settings, configure antivirus scan settings, FIM, application whitelist.
Security Reader	Internal	NP	Limited	Check compliance of cloud security configuration	Check compliance of cloud security configuration, including adherence to CIS benchmarks, security recommendations.



Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed
System Owner	Internal	P	Moderate	Break Glass account for tenancy and subscription configuration	Tenancy and subscription global settings that cannot be performed by a System Administrator role.

There are currently 6 internal personnel and 0 external personnel. Within one year, it is anticipated that there will be 6 internal personnel and 0 external personnel.

9.4 NETWORK ARCHITECTURE

Assessors should be able to easily map hardware, software, and network inventories back to this diagram. The logical network topology is shown in Figure 9-1 Network Diagram mapping the data flow between components. The following Figure 9-1 Network Diagram(s) provides a visual depiction of the system network components that constitute Enter Information System Abbreviation.

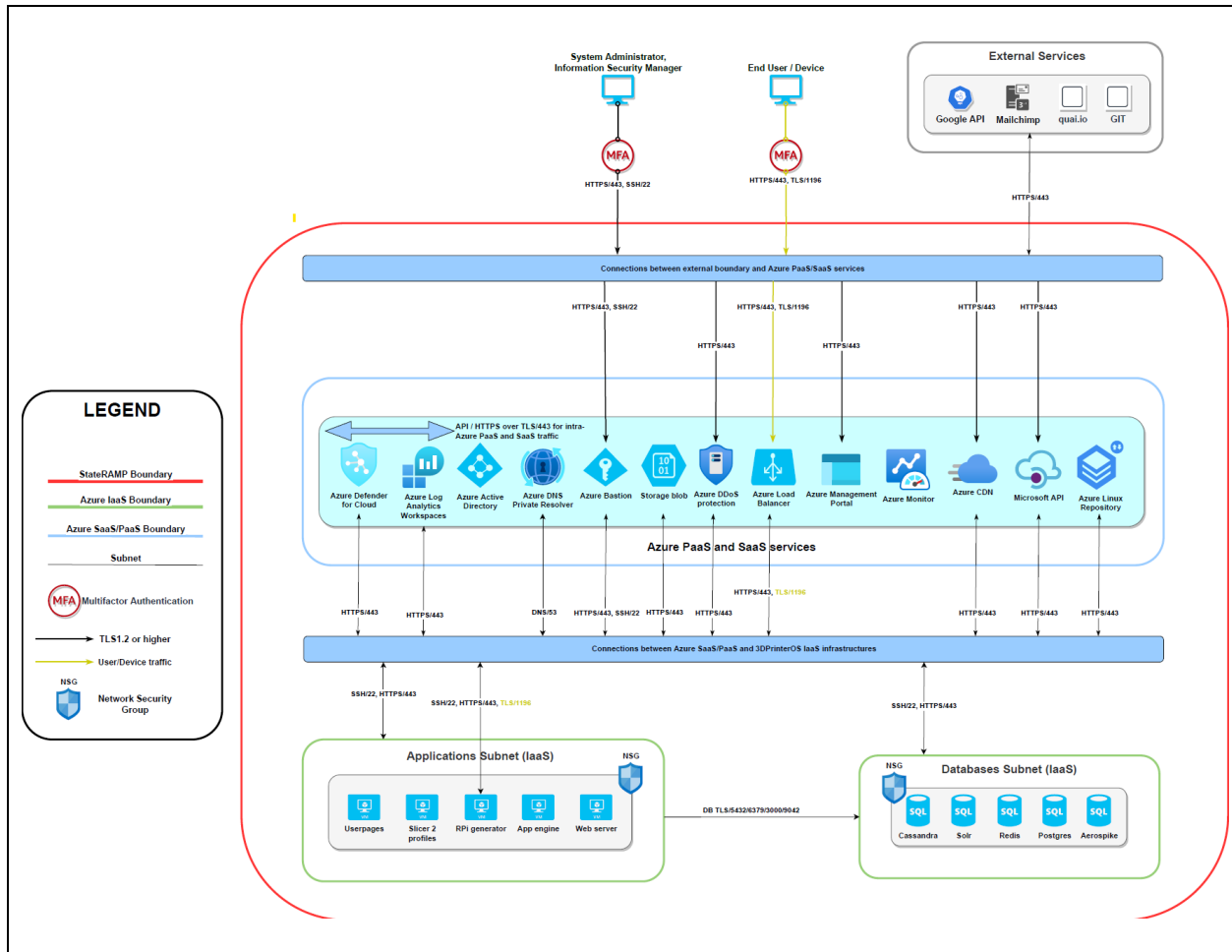


Figure 9-1 Network Diagram



9.5 DATA FLOW

The data flow in and out of the system boundaries is represented in Figure 9-2 Data Flow Diagram below.

Data into the boundary comprises standard inbound connection for HTTPS and API on TCP port 443 for both system and portal management. In addition, port 1196 is used for M2M communication with forward deployed client system that connects to 3D printers directly.

Outbound data flows all use TCP port 443 for integration with Mailchimp, Google API and quai.io.

Internal communication uses Azure Bastion host for management on both TCP ports 22 and 443, UDP port 53 for DNS resolution and various TCP ports for backend databases connection (5432, 6379, 3000, 9042).

All machines have individual NSG firewall attached to a network interface to achieve network microsegmentation objective.

Communication between boundaries and machines is restricted only to necessary network ports and adheres to “default deny” principle.

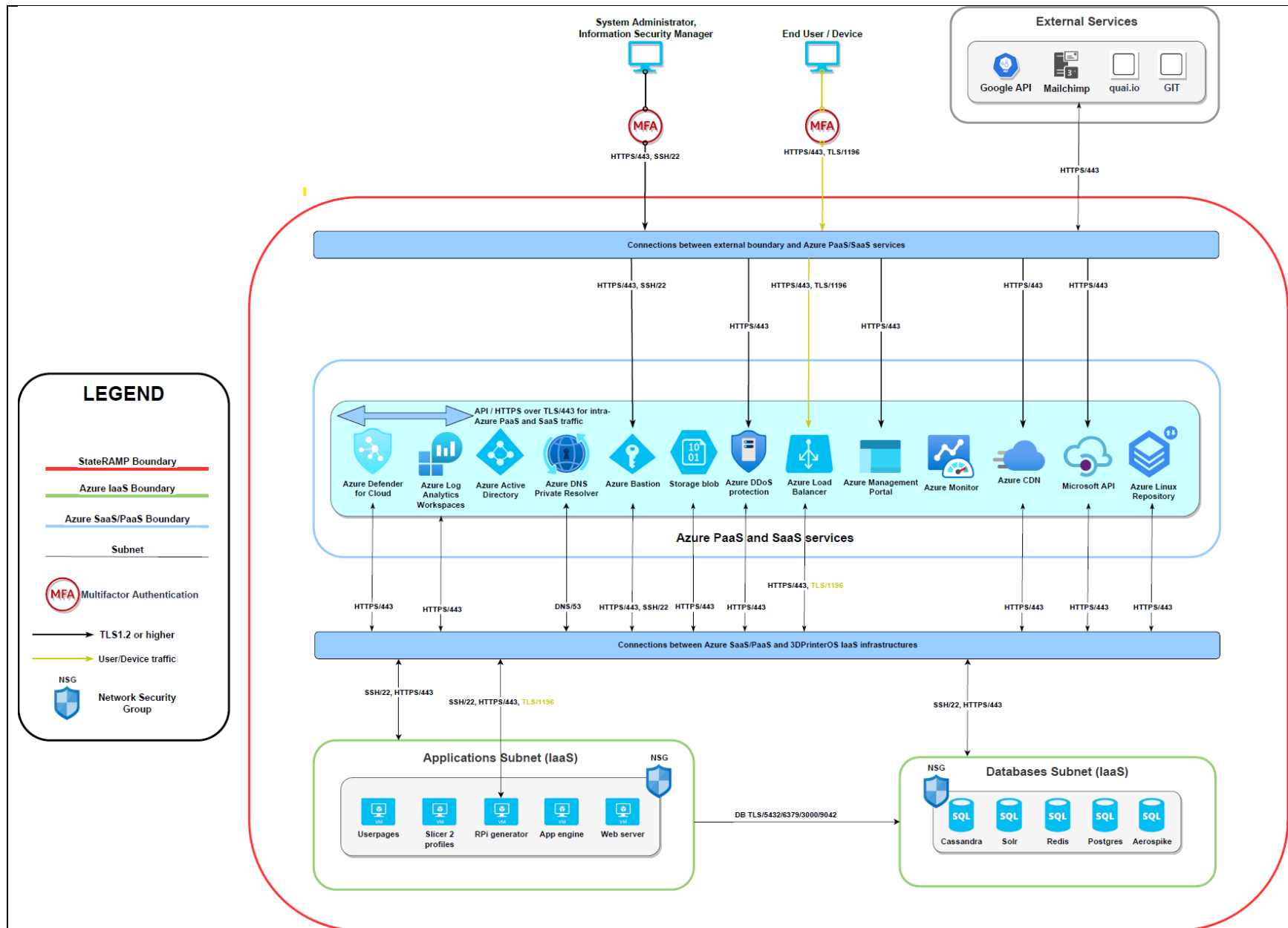




Figure 9-2 Data Flow Diagram

9.6 PORTS, PROTOCOLS AND SERVICES

Table 15 Ports, Protocols, and Services below lists the ports, protocols and services enabled in this information system.

Table 15 Ports, Protocols, and Services

Ports (TCP/UDP)*	Protocols	Services	Purpose	Used By
UDP 53	DNS	Network Name Resolution	Network Name Resolution for all services	All machines
TCP 443	TLS (for HTTPS and API)	Various web services	Web access, Azure Bastion	UserPages, Web Server
TCP 22	SSH	Secure Socket Shell	Machines management via shell	All machines backend connection from Azure Bastion
TCP 5432	PostgreSQL Database	PostgreSQL Database	Main relational database	Postgres from AppEngine
TCP 6379	Redis Database	Redis Database	Main in-memory cache database	Redis from AppEngine
TCP 3000	Aerospike Database	Aerospike Database	Multimodal database	Aerospike from AppEngine
TCP 9042	Cassandra Database	Cassandra Database	NoSQL database	Cassandra from AppEngine
TCP 1196	TCP, custom connection	RPi generator service	RPi generator connection for custom client	RPi generator

* Transmission Control Protocol (TCP), User Datagram Protocol (UDP)



10. SYSTEM INTERCONNECTIONS

Table 16. System Interconnections

SP* IP Address and Interface	External Organization Name and IP Address of System	External Point of Contact and Phone Number	Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.)**	Data Direction (incoming, outgoing, or both)	Information Being Transmitted	Port or Circuit Numbers
50.19.215.206 , 50.17.203.165 , 23.21.56.188 , 23.23.103.69	Quai.io	support@coreos.com +19193013003	TLS	Outgoing	Package updates	TCP 443
205.201.128.0/20, 198.2.128.0/18, 148.105.0.0/16	Mailchimp Mandrill	support@intuit.com +18003155939	TLS	Outgoing	Email communication with updates	TCP 443
34.74. 90.64/28, 34.74. 226.0/24	Gitlab	techsupport@gitlab.com Outbound calls only	TLS	Outgoing	GIT webhooks	TCP 443
IP addresses range: gstatic.com/ipranges/goog.json	Google API	googleadsapi-support@google.com (650) 253-0000	TLS	Outgoing	API statistics	TCP 443

*Service Processor

**Internet Protocol Security (IPSec), Virtual Private Network (VPN), Secure Sockets Layer (SSL)



11. MINIMUM SECURITY CONTROLS

Security controls must meet minimum security control baseline requirements. Upon categorizing a system as Category 1,2, or 3 the corresponding security control baseline standards apply. Some of the control baselines have enhanced controls which are indicated in parentheses.

Security controls that are representative of the sensitivity of 3DPrinterOS are described in the sections that follow. Security controls that are designated as “Not Selected” or “Withdrawn by NIST” are not described unless they have additional StateRAMP controls. Guidance on how to describe the implemented standard can be found in NIST 800-53, Rev 4. Control enhancements are marked in parentheses in the sensitivity columns.

A summary of which security standards pertain to which sensitivity level is found in Table 17. Summary of Required Security Controls that follows.

Table 17. Summary of Required Security Controls

ID	Control Description	Impact Level	
		Category 1	Category 3
AC			
	Access Control Policy and Procedures	AC-1	AC-1
	Account Management	AC-2	AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (12)
	Access Enforcement	AC-3	AC-3
	Information Flow Enforcement	Not Selected	AC-4 (21)
	Separation of Duties	Not Selected	AC-5
	Least Privilege	Not Selected	AC-6 (1) (2) (5) (9) (10)
	Unsuccessful Logon Attempts	AC-7	AC-7
	System Use Notification	AC-8	AC-8
	Concurrent Session Control	Not Selected	AC-10
	Session Lock	Not Selected	AC-11 (1)
	Session Termination	Not Selected	AC-12
	Permitted Actions Without Identification or Authentication	AC-14	AC-14
	Remote Access	AC-17	AC-17 (1) (2) (3) (4) (9)
	Wireless Access	AC-18	AC-18 (1)
	Access Control For Mobile Devices	AC-19	AC-19 (5)
	Use of External Information Systems	AC-20	AC-20 (1) (2)
	Information Sharing	Not Selected	AC-21
	Publicly Accessible Content	AC-22	AC-22
AT			



ID	Control Description	Impact Level	
		Category 1	Category 3
	Security Awareness and Training Policy and Procedures	AT-1	AT-1
	Security Awareness Training	AT-2	AT-2 (2)
	Role-Based Security Training	AT-3	AT-3
	Security Training Records	AT-4	AT-4
AU			
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1
AU-2	Audit Events	AU-2	AU-2 (3)
AU-3	Content of Audit Records	AU-3	AU-3 (1)
AU-4	Audit Storage Capacity	AU-4	AU-4
AU-5	Response to Audit Processing Failures	AU-5	AU-5
AU-6	Audit Review, Analysis and Reporting	AU-6	AU-6 (1) (3)
AU-7	Audit Reduction and Report Generation	Not Selected	AU-7 (1)
AU-8	Time Stamps	AU-8	AU-8 (1)
AU-9	Protection of Audit Information	AU-9	AU-9 (2) (4)
AU-10	Non-repudiation	Not Selected	Not Selected
AU-11	Audit Record Retention	AU-11	AU-11
AU-12	Audit Generation	AU-12	AU-12
CA			
CA-1	Security Assessment and Authorization Policies and Procedures	CA-1	CA-1
CA-2	Security Assessments	CA-2 (1)	CA-2 (1) (2) (3)
CA-3	System Interconnections	CA-3	CA-3 (3) (5)
CA-5	Plan of Action and Milestones	CA-5	CA-5
CA-6	Security Authorization	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7	CA-7 (1)
CA-8	Penetration Testing	Not Selected	CA-8 (1)
CA-9	Internal System Connections	CA-9	CA-9
CM			
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	Not Selected	CM-3 (2)
CM-4	Security Impact Analysis	CM-4	CM-4
CM-5	Access Restrictions For Change	Not Selected	CM-5 (1) (3) (5)
CM-6	Configuration Settings	CM-6	CM-6 (1)
CM-7	Least Functionality	CM-7	CM-7 (1) (2) (5)*
CM-8	Information System Component Inventory	CM-8	CM-8 (1) (3) (5)



ID	Control Description	Impact Level	
		Category 1	Category 3
CM-9	Configuration Management Plan	Not Selected	CM-9
CM-10	Software Usage Restrictions	CM-10	CM-10 (1)
CM-11	User-Installed Software	CM-11	CM-11
CP			
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1) (2) (3) (8)
CP-3	Contingency Training	CP-3	CP-3
CP-4	Contingency Plan Testing	CP-4	CP-4 (1)
CP-6	Alternate Storage Site	Not Selected	CP-6 (1) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7 (1) (2) (3)
CP-8	Telecommunications Services	Not Selected	CP-8 (1) (2)
CP-9	Information System Backup	CP-9	CP-9 (1) (3)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10 (2)
IA			
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	IA-2 (1) (12)	IA-2 (1) (2) (3) (5) (8) (11) (12)
IA-3	Device Identification and Authentication	Not Selected	IA-3
IA-4	Identifier Management	IA-4	IA-4 (4)
IA-5	Authenticator Management	IA-5 (1) (11)	IA-5 (1) (2) (3) (4) (6) (7) (11)
IA-6	Authenticator Feedback	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)
IR			
IR-1	Incident Response Policy and Procedures	IR-1	IR-1
IR-2	Incident Response Training	IR-2	IR-2
IR-3	Incident Response Testing	Not Selected	IR-3 (2)
IR-4	Incident Handling	IR-4	IR-4 (1)
IR-5	Incident Monitoring	IR-5	IR-5
IR-6	Incident Reporting	IR-6	IR-6 (1)
IR-7	Incident Response Assistance	IR-7	IR-7 (1) (2)
IR-8	Incident Response Plan	IR-8	IR-8
IR-9	Information Spillage Response	Not Selected	IR-9 (1) (2) (3) (4)
MA			



ID	Control Description	Impact Level	
		Category 1	Category 3
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1
MA-2	Controlled Maintenance	MA-2	MA-2
MA-3	Maintenance Tools	Not Selected	MA-3 (1) (2) (3)
MA-4	Nonlocal Maintenance	MA-4	MA-4 (2)
MA-5	Maintenance Personnel	MA-5	MA-5 (1)
MA-6	Timely Maintenance	Not Selected	MA-6
MP			
MP-1	Media Protection Policy and Procedures	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2
MP-3	Media Marking	Not Selected	MP-3
MP-4	Media Storage	Not Selected	MP-4
MP-5	Media Transport	Not Selected	MP-5 (4)
MP-6	Media Sanitization	MP-6	MP-6 (2)
MP-7	Media Use	MP-7	MP-7 (1)
PE			
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2
PE-3	Physical Access Control	PE-3	PE-3
PE-4	Access Control For Transmission Medium	Not Selected	PE-4
PE-5	Access Control For Output Devices	Not Selected	PE-5
PE-6	Monitoring Physical Access	PE-6	PE-6 (1)
PE-8	Visitor Access Records	PE-8	PE-8
PE-9	Power Equipment and Cabling	Not Selected	PE-9
PE-10	Emergency Shutoff	Not Selected	PE-10
PE-11	Emergency Power	Not Selected	PE-11
PE-12	Emergency Lighting	PE-12	PE-12
PE-13	Fire Protection	PE-13	PE-13 (2) (3)
PE-14	Temperature and Humidity Controls	PE-14	PE-14 (2)
PE-15	Water Damage Protection	PE-15	PE-15
PE-16	Delivery and Removal	PE-16	PE-16
PE-17	Alternate Work Site	Not Selected	PE-17
PE-18	Location of Information System Components	Not Selected	Not Selected
PL			
PL-1	Security Planning Policy and Procedures	PL-1	PL-1
PL-2	System Security Plan	PL-2	PL-2 (3)



ID	Control Description	Impact Level	
		Category 1	Category 3
PL-4	Rules of Behavior	PL-4	PL-4 (1)
PL-8	Information Security Architecture	Not Selected	PL-8
PS			
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1
PS-2	Position Risk Designation	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3 (3)
PS-4	Personnel Termination	PS-4	PS-4
PS-5	Personnel Transfer	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8
RA			
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3
RA-5	Vulnerability Scanning	RA-5	RA-5 (1) (2) (3) (5) (6) (8)
SA			
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2
SA-3	System Development Life Cycle	SA-3	SA-3
SA-4	Acquisition Process	SA-4 (10)	SA-4 (1) (2) (8) (9) (10)
SA-5	Information System Documentation	SA-5	SA-5
SA-8	Security Engineering Principles	Not Selected	SA-8
SA-9	External Information System Services	SA-9	SA-9 (1) (2) (4) (5)
SA-10	Developer Configuration Management	Not Selected	SA-10 (1)
SA-11	Developer Security Testing and Evaluation	Not Selected	SA-11 (1) (2) (8)
SA-12	Supply Chain Protection	Not Selected	Not Selected
SA-15	Development Process, Standards and Tools	Not Selected	Not Selected
SA-16	Developer-Provided Training	Not Selected	Not Selected
SA-17	Developer Security Architecture and Design	Not Selected	Not Selected
SC			
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1
SC-2	Application Partitioning	Not Selected	SC-2
SC-3	Security Function Isolation	Not Selected	Not Selected
SC-4	Information In Shared Resources	Not Selected	SC-4



ID	Control Description	Impact Level	
		Category 1	Category 3
SC-5	Denial of Service Protection	SC-5	SC-5
SC-6	Resource Availability	Not Selected	SC-6
SC-7	Boundary Protection	SC-7	SC-7 (3) (4) (5) (7) (8) (12) (13) (18)
SC-8	Transmission Confidentiality and Integrity	Not Selected	SC-8 (1)
SC-10	Network Disconnect	Not Selected	SC-10
SC-12	Cryptographic Key Establishment and Management	SC-12	SC-12 (2) (3)
SC-13	Cryptographic Protection	SC-13	SC-13
SC-15	Collaborative Computing Devices	SC-15	SC-15
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17
SC-18	Mobile Code	Not Selected	SC-18
SC-19	Voice Over Internet Protocol	Not Selected	SC-19
SC-20	Secure Name / Address Resolution Service (Authoritative Source)	SC-20	SC-20
SC-21	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	SC-21	SC-21
SC-22	Architecture and Provisioning for Name / Address Resolution Service	SC-22	SC-22
SC-23	Session Authenticity	Not Selected	SC-23
SC-24	Fail in Known State	Not Selected	Not Selected
SC-28	Protection of Information At Rest	Not Selected	SC-28 (1)
SC-39	Process Isolation	SC-39	SC-39
SI			
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1
SI-2	Flaw Remediation	SI-2	SI-2 (2) (3)
SI-3	Malicious Code Protection	SI-3	SI-3 (1) (2) (7)
SI-4	Information System Monitoring	SI-4	SI-4 (1) (2) (4) (5) (14) (16) (23)
SI-5	Security Alerts, Advisories and Directives	SI-5	SI-5
SI-6	Security Function Verification	Not Selected	SI-6
SI-7	Software, Firmware, and Information Integrity	Not Selected	SI-7 (1) (7)
SI-8	Spam Protection	Not Selected	SI-8 (1) (2)
SI-10	Information Input Validation	Not Selected	SI-10
SI-11	Error Handling	Not Selected	SI-11
SI-12	Information Handling and Retention	SI-12	SI-12
SI-16	Memory Protection	SI-16	SI-16



The definitions in Table 18. Control Origination and Definitions indicate where each security control originates.

Table 18. Control Origination and Definitions

Control Origination	Definition	Example
Service Provider Corporate	A control that originates from the CSP Name corporate network.	DNS from the corporate network provides address resolution services for the information system and the service offering.
Service Provider System Specific	A control specific to a particular system at the CSP Name and the control is not part of the standard corporate controls.	A unique host-based intrusion detection system (HIDS) is available on the service offering platform but is not available on the corporate network.
Service Provider Hybrid	A control that makes use of both corporate controls and additional controls specific to a particular system at the CSP Name.	There are scans of the corporate network infrastructure; scans of databases and web-based application are system specific.
Configured by Customer	A control where the customer needs to apply a configuration in order to meet the control requirement.	User profiles, policy/audit configurations, enabling/disabling key switches (e.g., enable/disable http* or https, etc.), entering an IP range specific to their organization are configurable by the customer.
Provided by Customer	A control where the customer needs to provide additional hardware or software in order to meet the control requirement.	The customer provides a SAML SSO solution to implement two-factor authentication.
Shared	A control that is managed and implemented partially by the CSP Name and partially by the customer.	Security awareness training must be conducted by both the CSPN and the customer.
Inherited from pre-existing StateRAMP Authorization	A control that is inherited from another CSP Name system that has already received a StateRAMP Authorization.	A PaaS or SaaS provider inherits PE controls from an IaaS provider.



12. SYSTEM SECURITY PLAN ATTACHMENTS

A recommended attachment file naming convention is **<information system abbreviation> <attachment identifier> <document abbreviation> <version number>** (for example, "Information System Abbreviation A8 IRP v1.0"). Use this convention to generate names for the attachments. Enter the appropriate file names and file extensions in Table 19 to describe the attachments provided. Make only the following additions/changes to Table 19:

- The first item, Information Security Policies and Procedures (ISPP) may be fulfilled by multiple documents. If that is the case, add lines to Table 19. to differentiate between them using the "xx" portion of the File Name. Enter Information System Abbreviation A1 ISPP xx v1.0. Delete the "xx" if there is only one document.
- Enter the file extension for each attachment.
- Do not change the Version Number in the File Name in Table 19. Names of Provided Attachments. (Information System Abbreviation, attachment number, document abbreviation, version number)

Table 19. Names of Provided Attachments

Attachment	File Name	StateRAMP Template Required?
TX-RAMP SSP Workbook (Includes Control Implementations, CIS Matrix, Inventory Workbook, Laws & Regulations)	3DPrinterOS_SSP_A_WB_V1.1_20250130.xlsx	Yes
Information Security Policies	3DPrinterOS_AC_POL_V1.2_20240115.pdf 3DPrinterOS_AT_POL_V1.2_20240115.pdf 3DPrinterOS_AU_POL_V1.2_20240115.pdf 3DPrinterOS_CA_POL_V1.2_20240115.pdf 3DPrinterOS_CM_POL_V1.2_20240115.pdf 3DPrinterOS_CP_POL_V1.2_20240115.pdf 3DPrinterOS_IA_POL_V1.2_20240115.pdf 3DPrinterOS_IR_POL_V1.2_20240115.pdf 3DPrinterOS_MA_POL_V1.2_20240115.pdf 3DPrinterOS_MP_POL_V1.2_20240115.pdf 3DPrinterOS_PE_POL_V1.2_20240115.pdf 3DPrinterOS_PL_POL_V1.2_20240115.pdf 3DPrinterOS_PS_POL_V1.2_20240115.pdf 3DPrinterOS_RA_POL_V1.2_20240115.pdf 3DPrinterOS_SA_POL_V1.2_20240115.pdf 3DPrinterOS_SC_POL_V1.2_20240115.pdf 3DPrinterOS_SI_POL_V1.2_20240115.pdf	No
Information Security Procedures	3DPrinterOS_AC_PROC_V1.2_20240115.pdf 3DPrinterOS_AT_PROC_V1.2_20240115.pdf 3DPrinterOS_AU_PROC_V1.2_20240115.pdf 3DPrinterOS_CA_PROC_V1.2_20240115.pdf 3DPrinterOS_CM_PROC_V1.2_20240115.pdf	No



Attachment	File Name	StateRAMP Template Required?
	3DPrinterOS_CP_PROC_V1.2_20240115.pdf 3DPrinterOS_IA_PROC_V1.2_20240115.pdf 3DPrinterOS_IR_PROC_V1.2_20240115.pdf 3DPrinterOS_MA_PROC_V1.2_20240115.pdf 3DPrinterOS_MP_PROC_V1.2_20240115.pdf 3DPrinterOS_PE_PROC_V1.2_20240115.pdf 3DPrinterOS_PL_PROC_V1.2_20240115.pdf 3DPrinterOS_PS_PROC_V1.2_20240115.pdf 3DPrinterOS_RA_PROC_V1.2_20240115.pdf 3DPrinterOS_SA_PROC_V1.2_20240115.pdf 3DPrinterOS_SC_PROC_V1.2_20240115.pdf 3DPrinterOS_SI_PROC_V1.2_20240115.pdf	
Configuration Management Plan	3DPrinterOS_SSP_A_CMP_1.0_20240603.pdf	Yes
Information System Contingency Plan	3DPrinterOS_SSP_A_ISCP_V1.0_20240604.pdf	Yes
Incident Response Plan	3DPrinterOS_SSP_A_IRP_V1.0_20240606.pdf	Yes
Rules of Behavior	3DPrinterOS_SSP_A_ROB_V1.1_20240529.pdf	Yes
Separation of Duties Matrix	3DPrinterOS_SSP_A_SDM_V1.0_20240608.xlsx	No
User Guide	Web - based documentation by topic: 3DPrinterOS Knowledge Base (helpdocs.io)	No
Continuous Monitoring Plan	3DPrinterOS_SSP_A_ISCM_V1.0_20240607.pdf	Yes
Supplemental Letter for Authorized IaaS/PaaS	Supplemental Letter for Authorized IaaSPaaS.pdf	No



13. DIGITAL IDENTITY WORKSHEET

The Digital Identity section explains the objective for selecting the appropriate Digital Identity levels for the candidate system. Guidance on selecting the system authentication technology solution is available in NIST SP 800-63, Revision 3, Digital Identity Guidelines.

13.1 INTRODUCTION AND PURPOSE

This document provides guidance on digital identity services (Digital Identity, which is the process of establishing confidence in user identities electronically presented to an information system). Authentication focuses on the identity proofing process (IAL), the authentication process (AAL), and the assertion protocol used in a federated environment to communicate authentication and attribute information (if applicable) (FAL).

NIST SP 800-63-3, Digital Identity Guidelines, does not recognize the four Levels of Assurance model previously used by federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels corresponding to each function being performed. NIST SP 800-63-3 can be found at the following URL: [NIST SP 800-63-3](#).

13.2 INFORMATION SYSTEM NAME/TITLE

This Digital Identity Plan provides an overview of the security requirements for the 3DPrinterOS in accordance with NIST SP 800-63-3.

Table 20. Information System Name and Title

Unique Identifier	Information System Name	Information System Abbreviation
TX1071880		3DPrinterOS

13.3 DIGITAL IDENTITY LEVEL DEFINITIONS

NIST SP 800-63-3 defines three levels in each of the components of identity assurance to categorize a federal information system's Digital Identity posture. NIST SP 800-63-3 defines Digital Identity levels below. StateRAMP maps its system categorization levels to NIST 800-63-3's levels as shown in Table 21.

- IAL – refers to the identity proofing process.
- AAL – refers to the authentication process.
- FAL – refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to a relying party (RP).



Table 21. Mapping StateRAMP Levels to NIST SP 800-63-3 Levels

StateRAMP System Categorization	Identity Assurance Level (IAL)	Authenticator Assurance Level (AAL)	Federation Assurance Level (FAL)
High	IAL3: In-person, or supervised remote identity proofing	AAL3: Multi-factor required based on hardware-based cryptographic authenticator and approved cryptographic techniques	FAL3: The subscriber (user) must provide proof of possession of a cryptographic key, which is referenced by the assertion. The assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it
Category 3	IAL2: In-person or remote, potentially involving a “trusted referee”	AAL2: Multi-factor required, using approved cryptographic techniques	FAL2: Assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it
Category 1	IAL1: Self-asserted	AAL1: Single-factor or multi-factor	FAL1: Assertion is digitally signed by the identity provider

Selecting the appropriate Digital Identity level for a system enables the system owner to determine the right system authentication technology solution for the selected Digital Identity levels. Guidance on selecting the system authentication technology solution is available in NIST SP 800-63-3.

13.4 REVIEW MAXIMUM POTENTIAL IMPACT LEVELS

3D Control Systems has assessed the potential risk from Digital Identity errors, or Digital Identity misuse, related to a user’s asserted identity. 3D Control Systems has taken into consideration the potential for harm (impact) and the likelihood of the occurrence of the harm and has identified an impact profile as found in Table 22. Potential Impacts for Assurance Levels.

Assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Table 22. Potential Impacts for Assurance Levels

Potential Impact Categories	Assurance Level Impact Profile		
	1	2	3
Inconvenience, distress, or damage to standing or reputation	Category 1	Category 3	High
Financial loss or agency liability	Category 1	Category 3	High
Harm to agency programs or public interests	N/A	Category 1/3	High
Unauthorized release of sensitive information	N/A	Category 1/3	High
Personal Safety	N/A	Category 1	Mod/High



Potential Impact Categories	Assurance Level Impact Profile		
	1	2	3
Civil or criminal violations	N/A	Category 1/3	High

13.5 DIGITAL IDENTITY LEVEL SELECTION

The 3D Control Systems has identified that they support the Digital Identity Level that has been selected for the 3DPrinterOS as noted in Table 23. Digital Identity Level. The selected Digital Identity Level indicated is supported for federal agency consumers of the cloud service offering. Implementation details of the Digital Identity mechanisms are provided in the System Security Plan under control IA-2.

Table 23. Digital Identity Level

Digital Identity Level	Maximum Impact Profile	Selection
Level 1: AAL1, IAL1, FAL1	Category 1	<input checked="" type="checkbox"/>
Level 2: AAL2, IAL2, FAL2	Category 3	<input type="checkbox"/>
Other		



14. PTA AND PIA

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and if necessary, the Privacy Impact Assessment (PIA) attachment, which will be reviewed for quality. The PTA is included in this section, and the PIA Template can be found on the StateRAMP website. The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues.

14.1 PRIVACY OVERVIEW AND POINT OF CONTACT (POC)

The Table 24. Information System Name; Privacy POC individual is identified as the Information System Name; Privacy Officer and POC for privacy at CSP Name.

Table 24. Information System Name; Privacy POC

Name	Michailas Ornovskis
Title	Chief Information Security Officer
CSP / Organization	3D Control Systems
Address	340 S Lemon Ave #9734, Walnut, CA 91789, USA
Phone Number	+3725017350
Email Address	michailas@3dprinterOS.com



14.2 PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally Identifiable Information (PII) as defined in OMB Memorandum M-07-16 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Information that could be tied to more than one person (date of birth) is not considered PII unless it is made available with other types of information that together could render both values as PII (for example, date of birth and street address). A non-exhaustive list of examples of types of PII includes:

- Social Security numbers
- Passport numbers
- Driver's license numbers
- Biometric information
- DNA information
- Bank account numbers
- Voice recordings

PII refers to information that can be traced back to an individual person.

14.3 PRIVACY DESIGNATION

Service providers perform an annual analysis to determine if PII is collected by any of the system components. Clouds that do not collect PII and would like to opt-out of hosting privacy information may elect to do so and are not required to fill out the Privacy Impact Assessment Questions. If a CSP is willing to host PII, the Privacy Impact Assessment Questions should be answered given the current knowledge of the CSP. A CSP is not required to solicit customers for the information.

Cloud customers (data owner/system owners) are required to perform their own Privacy Impact Assessments and may share this information with the CSP if they so desire (for informational purposes and/or to work with the CSP to develop processes and procedures for managing their PII).

14.4 THRESHOLD ANALYSIS

Check one.

<input checked="" type="checkbox"/>	Opt-out. This cloud will not host privacy information (No privacy related information apart from the one used for customer login is stored).
<input type="checkbox"/>	This cloud is willing to host privacy information. Select the cloud layers that are represented by 3DPrinterOS. Select all that apply.
<input checked="" type="checkbox"/>	This cloud includes Software as a Service (SaaS).
<input type="checkbox"/>	This cloud includes Platform as a Service (PaaS).
<input type="checkbox"/>	This cloud includes Infrastructure as a Service (IaaS).

14.5 PRIVACY IMPACT ASSESSMENT TALKING POINTS

According to NIST SP 800-122, Appendix D, there must be no personal data record-keeping systems whose very existence is secret. Additionally, NIST SP 800-122, Appendix D states, "There should be a



general policy of openness about developments, practices, and policies with respect to personal data.” Means should be readily available to establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.

In light of the NIST guidance, Privacy Impact Assessment talking points have been developed for the purpose of ensuring full disclosure between stakeholders. Identifiers in parenthesis after a section title indicate NIST SP 800-53, controls that are related to the particular talking point. These mapping to Appendix J privacy controls are not considered a replacement for Appendix J controls.

14.6 PII MAPPING OF COMPONENTS (SE-1, DM-1)

3DPrinterOS consists of 3 key components. Each component has been analyzed to determine if any elements of that component collect and/or store PII. The type of PII collected and/or stored by System Name and the functions that collect it are recorded in Table 25.

Table 25 PII Mapped to Components

Components	Does this Component Collect or Store PII? (Yes/No)	Type of PII	Reason for Collection of PII	Safeguards
livedb-aerospike-1	Yes	SAML login information, username and email	Authentication, user mapping	Database encryption, access control, backups
livedb2-pgsql-1	Yes	SAML login information, username and email	Authentication, user mapping	Database encryption, access control, backups
livedb2-redis-1	Yes	SAML login information, username and email	Authentication, user mapping	Database encryption, access control, backups



14.7 PROSPECTIVE PII USE

Respond to the following questions:

1. Are there any data fields in the platform or application that have been targeted for the collection or storage of PII? If yes, please name those fields. (SE-1, DM-1, IP-1)		
Data fields that are filled with SAML federation information. According to StateRAMP description, if the PII information is only used for login, this is an opt-out situation.		
If PII fields are used, can individuals “opt-out” of PII fields by declining to provide PII or by consenting only to a particular use (e.g., allowing basic use of their personal information, but not sharing with other government agencies)? (IP-1)		
Click here to enter explanation.		
<input checked="" type="checkbox"/>	Yes	Explain the circumstances of being able to opt-out of PII fields (either for specific data elements or specific uses of the data). (IP-1)
		It is possible to opt-out from marketing cookies.
<input type="checkbox"/>	No	It is not possible to opt-out.

14.8 SOURCES OF PII AND PURPOSE

1. Does CSP Name have knowledge of existing federal agencies that provide PII that gets imported into the system? (AP-2)

We don't deal with federal agencies in our system.

2. Has any agency that is known to provide PII to the system provided a stated purpose for populating the system with PII? (AP-1, AP-2)

No.

3. Does CSP Name currently populate the system with PII? If yes, where does the PII come from and what is the purpose? (AP-1, AP-2)

No, apart from SAML assertion from customer IdP systems (such as Microsoft Entra).

4. Will any third-party sources be providing PII that will be imported into the system (if known)? Please explain. (AP-1, AP-2)

No.

14.9 ACCESS TO PII AND SHARING

1. What third-party organizations will have access to the PII (if known)? Who establishes the criteria for what PII can be shared? (AP-1, AP-2, AR-8, IP-1, UL-2)

None.

2. What CSP Name personnel roles will have access to PII fields (e.g., users, managers, system administrators, developers, contractors, other)? Explain the need for CSP Name personnel to have access to the PII. (AR-8, UL-2)



Database Administrators only.

3. For CSP support staff, how is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access to PII require manager approval? (IP-2)

Change ticket and CMB approval is needed to access production database.

4. Do other systems that interconnect to the system share, transmit, or access the PII in the system? If yes, explain the purpose for system to system transmission, access, or sharing of PII. (UL-2)

No.

14.10 PII SAFEGUARDS AND LIABILITIES

1. What controls are in place to prevent the misuse (e.g., browsing) of PII by those having access? (AR-2)

Strong access control, processes and database encryption.

2. Who will be responsible for protecting the privacy rights of the individuals whose PII is collected, maintained, or shared on the system? Have policies and/or procedures been established for this responsibility and accountability? (AR-1, AR-2)

CISO and Information Security Manager are responsible.

3. Does the CSP Name provide annual security training include privacy training? Does CSP Name require their contractors that have access to the PII to take the training? (AR-5)

Yes, this is part of the regular security training.

4. Who is privacy officer responsible for assuring safeguards for the PII? (AR-1)

CISO role.

5. What is the magnitude of harm to the individuals if privacy related data is disclosed, intentionally or unintentionally? (AR-2)

Limited, since the only PII data used is coming from IdP for login purposes.

6. What involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system? (AR-3)

We don't have contractors.

7. Is the PII owner advised about what federal agencies or other organizations share or have access to the data? (AR-1)

None of them do and they have never asked.



14.11 CONTRACTS, AGREEMENTS, AND OWNERSHIP

1. NIST SP 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this accountability described in contracts with customers? Why or why not? (AR-3)

This is part of the agreement and privacy policy.

2. Do contracts with customers establish who has ownership rights over data including PII? (AR-2, AR-3)

Always the customer.

3. Do contracts with customers require that customers notify CSP Name if the customer intends to populate the service platform with PII? Why or why not? (AR-3)

There is no population apart from IdP assertion.

4. Do CSP Name contracts with customers establish record retention responsibilities for both the customer and CSP Name? (AR-2, AR-3)

Yes.

5. Is the degree to which CSP Name will accept liability for exposure of PII clearly defined in agreements with customers? (AR-3)

To the extent covered in the legislation, since 3D Control Systems is the Data Processor.

14.12 ACCURACY OF THE PII AND REDRESS

1. Is the PII collected verified for accuracy? Why or why not? (DI-1)

We consider IdP as “source of truth” and trust its accuracy.

2. Is the PII current? How is this determined? (DI-1)

Synchronization occurs every time SAML assertion happens.

3. Is there a process for individuals to have inaccurate PII that is maintained by the system corrected or amended, as appropriate?

Yes, it is possible through organization superuser (customer role for administering their tenant).

14.13 MAINTENANCE AND ADMINISTRATIVE CONTROLS

1. If the system is operated in more than one site, how is consistent use of the PII maintained in all sites? Are the same controls used?

System operates in one site at a time.

2. What are the retention periods of PII for this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines? (AR-2, AR-3, DM-2)



Customer defines the retention. Since PII data is only used for login, it is stored for as long contractual obligation demands. After the contract expires, data is deleted within three months. At any point of time customer can request data extraction or deletion from the system.

3. What are the procedures for disposition of the PII at the end of the retention period? How long will any reports that contain PII be maintained? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)? Who establishes the decommissioning procedures? (AR-2, DM-2)

Reports don't contain PII. Data deletion from the database is irreversible procedure.

4. Is the system using new technologies that contain PII in ways that have not previously deployed? (e.g., smart cards, caller-ID, biometrics, PIV cards, etc.)?

No.

5. How does the use of this technology affect privacy? Does the use of this technology introduce compromise that did not exist prior to the deployment of this technology?

N/A.

6. Is access to the PII being monitored, tracked, or recorded? (AR-4)

Yes.

7. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision? (TR-2)

N/A.

14.14 BUSINESS PROCESSES AND TECHNOLOGY

1. Have the talking points found herein resulted in circumstances that requires changes to business processes?

No.

2. Does the outcome of these talking points require that technology or operational changes be made to the system?

No.

14.15 PRIVACY POLICY

1. Is there a system privacy policy and is it provided to all individuals whose PII you collect, maintain or store? (IP-1, TR-1, TR-3)

Yes.


2. Is the privacy policy publicly viewable? If yes, provide the URL. (TR-1, TR-3)

Yes, [3DPrinterOS Privacy Policy: Your Data Protection Guarantee](#)



14.16 SIGNATURES

The information found herein has been documented by *3D Control Systems* and has been reviewed by the CSP Name, Chief Privacy Officer for accuracy.

Chief Information Security Officer (in role of DPO) Signature			
			
Name	Michailas Ornovskis	Date	6/2/2024



15. SECURITY CATEGORIZATION

This document is intended to be used by state governments and procurement officials as a tool for determining the appropriate StateRAMP or FedRAMP security requirements in a request for proposal (RFP) with the intent of procuring a service provider using or offering IaaS, SaaS, and/or PaaS solutions that process, store, and/or transmit government data including PII, PHI, and/or PCI.

According to the Federal Information Security Management Act (FISMA) requirements, there are three distinct security objectives for information and information systems: confidentiality, integrity, and availability. These standards are used as the foundation to ensure service providers are providing solutions that meet the minimum-security requirements to process, store, and transmit certain types of government data.

It is necessary for States to accurately determine their required security baseline prior to publishing an RFP so that the State can select a service provider that meets the State's needs and provides the appropriate security controls to protect the State's data. This data classification self-assessment is based on the NIST 800-53 Revision 4 requirements and designed to help state and local governments easily identify the appropriate StateRAMP security category to include in an RFP.

15.1 INSTRUCTIONS

Answer the questions in the survey section to determine what StateRAMP security category requirements you need to include in your RFP to ensure your data is protected. Because of the level of reciprocity between StateRAMP and FedRAMP, a StateRAMP Category 1 requirement is equivalent to a FedRAMP Low Impact and a StateRAMP Category 3 requirement is equivalent to a FedRAMP Moderate Impact.

15.2 SURVEY QUESTIONS

5. Will the service provider process, transmit, and/or store non-sensitive State data, metadata, and/or data that may be released to the public that requires no additional levels of protection?
 - a. If yes, StateRAMP Category 1 is required.

No.

6. Will the service provider process, transmit, and/or store personally identifiable information (PII) as defined by the U.S. Department of Labor (DOL)?
 - a. If yes, StateRAMP Category 3 is required.

No.

7. Will the service provider process, transmit, and/or store protected health information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA)?
 - a. If yes, StateRAMP Category 3 is required.

No.



8. Will the service provider process, transmit, and/or store payment card industry (PCI) data as defined by the PCI Security Standards Council (PCI SSC)?

a. If yes, StateRAMP Category 3 is required.

No.

9. Will the loss or unavailability of the data that is processed, transmitted, and/or stored by the service provider result in a disruption to government operations?

a. If yes, StateRAMP Category 3 is required.

No.

10. Will the loss or unavailability of the data that is processed, transmitted, and/or stored by the service provider result in a loss of confidence or trust in the government?

a. If yes, StateRAMP Category 3 is required.

No.

11. Will the service provider process, transmit, and/or store criminal justice information (CJI), foreign affairs information, federal critical infrastructure information, national security information, and/or global trade information?

a. If yes, FedRAMP High Impact is required.

No.







DremelDigiLab_StCharlestR-VISchoolDistrict_14-State_OHG_VendorSigned

Final Audit Report

2025-07-15

Created:	2025-07-15
By:	Keith Perham (kperham@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA616SGbThwEL1EMlvNcAyo9sAVCqLHes9

"DremelDigiLab_StCharlestR-VISchoolDistrict_14-State_OHG_VendorSigned" History

-  Document created by Keith Perham (kperham@tec-coop.org)
2025-07-15 - 8:30:30 PM GMT
-  Document emailed to dtaylor@stcharlessd.org for signature
2025-07-15 - 8:32:28 PM GMT
-  Email viewed by dtaylor@stcharlessd.org
2025-07-15 - 8:36:08 PM GMT
-  Signer dtaylor@stcharlessd.org entered name at signing as David Taylor
2025-07-15 - 8:39:16 PM GMT
-  Document e-signed by David Taylor (dtaylor@stcharlessd.org)
Signature Date: 2025-07-15 - 8:39:18 PM GMT - Time Source: server
-  Agreement completed.
2025-07-15 - 8:39:18 PM GMT