Version 2.0 Agreement Approved: June 2019

DATA PRIVACY AGREEMENT (DPA)
FOR TEXAS K-12 INSTITUTIONS

Lackland ISD 02/23/2021

LEA NAME [Box 1] DATE [Box 2]

and

Labster Inc. 12/10/2020

OPERATOR NAME [Box 3] DATE [Box 4]

Background and Instructions

History of Agreement- This agreement has been drafted by the Texas Student Privacy Alliance (TXSPA). The Alliance is a collaborative group of Texas school districts that share common concerns around student and data privacy. The Texas K-12 CTO Council is the organization that sponsors the TXSPA and the TXSPA is the Texas affiliate of the national Student Data Privacy Consortium (SDPC). The SDPC works with other state alliances by helping establish common data privacy agreements unique to the jurisdiction of each state. This Texas agreement was drafted specifically for K-12 education institutions and included broad stakeholder input from Texas school districts, statewide associations such as TASB, TASA, and TASBO, and the Texas Education Agency. The purpose of this agreement is to set standards of both practice and expectations around data privacy such that all parties involved have a common understanding of expectations. This agreement also provides a mechanism (Exhibit E- General Offer of Terms) that would allow an Operator to extend the ability of other Texas school districts to be covered under the terms of the agreement should an Operator sign Exhibit E. This mechanism is intended to create efficiencies for both Operators and LEAs and generally enhance privacy practices and expectations for K-12 institutions and for companies providing services to K-12 institutions.

Instructions for Operators: This agreement is intended to be provided to an Operator from a LEA. The Operator should fully read the agreement and is requested to complete the below areas of the agreement. Once the Operator accepts the terms of the agreement, the Operator should wet sign the agreement and return it to the LEA. Once the LEA signs the agreement, the LEA should provide a signed copy of the agreement to the Operator.

Article/Exhibit	Box #	Description
Cover Page	Box # 3	Official Name of Operator
Cover Page	Box # 4	Date Signed by Operator
Recitals	Box #5	Contract Title for Service Agreement
Recitals	Box #6	Date of Service Agreement
Article 7	Boxes #7-10	Operator's designated representative
Signature Page	Boxes #15-19	Authorized Operator's representative signature
Exhibit A	Box #25	Description of services provided
Exhibit B	All Applicable Boxes	• Operator notates if data is collected to provide the described services. • Defines the schedule of data required for the Operator to provide the services outlined in Exhibit A
Exhibit D	All Applicable Boxes	(Optional Exhibit): Defines deletion or return of data expectations by LEA

Exhibit E	All Applicable Boxes	(Optional Exhibit): Operator may, by signing the Form of General Offer of Privacy Terms (General Offer, attached as Exhibit E), be bound by the terms of this DPA to any other Subscribing LEA who signs the acceptance in said Exhibit.
Exhibit F	Boxes # 25-29	A list of all Subprocessors used by the Operator to perform functions pursuant to the Service Agreement, list security programs and measures, list Operator's security measures

Instructions for LEA and/or Subscribing LEA: This agreement is intended to be provided to an Operator from a LEA. Upon receiving an executed agreement from an Operator, the LEA should fully review the agreement and if agreeable, should have an authorized LEA contact wet sign the agreement. Once signed by both the Operator and LEA, the LEA should send a copy of the signed agreement to the Operator.

Article/Exhibit	Box #	Description
Cover Page	Box # 1	Official Name of LEA
Cover Page	Box #2	Date Signed by LEA
Article 7	Boxes #11-14	LEA's designated representative
Signature Page	Boxes #20-24	Authorized LEA representative's signature
Exhibit D	All Applicable Boxes	(Optional Exhibit): Defines deletion or return of data expectations by LEA
Exhibit E	All Applicable Boxes	(Optional Exhibit) Only to be completed by a Subscribing LEA

RECITALS

WHEREAS, the Operator has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") according to a contract titled "Labster Inc." [Box 5] and dated 12/10/20 [Box 6] (tbe "Service Agreement"), and

WHEREAS, in order to provide the Services described in the Service Agreement, the Operator may receive or create and the LEA may provide documents or data that are covered by federal statutes, among them, the Federal Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506, and Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Operator's Services are also subject to state student privacy laws, including Texas Education Code Chapter 32; and

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

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

ARTICLE I: PURPOSE AND SCOPE

1. **Nature of Services Provided.** The Operator has agreed to provide digital educational services as outlined in Exhibit A and the Agreement.

2. **Purpose of DPA**. For Operator to provide services to the LEA it may become necessary for the LEA to share certain LEA Data. This DPA describes the Parties' responsibilities to protect Data.

3. **Data to Be Provided**. In order for the Operator to perform the Services described in the Service Agreement, LEA shall provide the categories of data described in the Schedule of Data, attached as Exhibit B.

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

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Ownership of Data**. All Data transmitted to the Operator pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Operator further acknowledges and agrees that all copies of such Data transmitted to the Operator, 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 Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Data contemplated per the Service Agreement shall remain the exclusive property of the LEA.

2. **Operator Materials**. Operator retains all right, title and interest in and to any and all of Operator's software, materials, tools, forms, documentation, training and implementation materials and intellectual property ("Operator Materials"). Operator grants to the LEA a personal, nonexclusive license to use the Operator Materials for its own non-commercial, incidental use as set forth in the Service Agreement. Operator represents that it has all intellectual property rights necessary to enter into and perform its obligations in this DPA and the Service Agreement, warrants to the District that the District will have use of any intellectual property contemplated by the Service Agreement free and clear of claims of any nature by any third Party including, without limitation, copyright or patent infringement claims, and agrees to indemnify the District for any related claims.

3. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Data on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Operator shall respond in a reasonably timely manner (and no later than 28 days from the date of the request) to the LEA's request for Data in a pupil's records held by the Operator to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Operator to review any of the Data accessed pursuant to the Services, the Operator shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

4. **Data Portability**. Operator shall, at the request of the LEA, make Data available including Pupil Generated Content in a readily accessible format.

5. **Third Party Request**. Should a Third Party, including law enforcement or a government entity, contact Operator with a request for data held by the Operator pursuant to the Services, the Operator shall immediately (within 1 business day), and to the extent legally permitted, redirect the Third Party to request the data directly from the LEA, notify the LEA of the request, and provide a copy of the request to the LEA. Furthermore, if legally permissible, Operator shall promptly notify the LEA of a subpoena compelling disclosure to a Third Party and provide a copy of the subpoena with sufficient time for the LEA to raise objections to the subpoena. The Operator will not use, disclose, compile, transfer, or sell the Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Data and/or any portion thereof. Notwithstanding any provision of this DPA or Service Agreement to the contrary, Operator understands that the LEA is subject to and will comply with the Texas Public Information Act (Chapter 552, Texas Government Code). Operator understands and agrees that information, documentation and other material in connection with the DPA and Service Agreement may be subject to public disclosure.

6. **No Unauthorized Use**. Operator shall use Data only for the purpose of fulfilling its duties and obligations under the Service Agreement and will not share Data with or disclose it to any Third Party without the prior written consent of the LEA, except as required by law or to fulfill its duties and obligations under the Service Agreement.

7. **Subprocessors**. All Subprocessors used by the Operator to perform functions pursuant to the Service Agreement shall be identified in Exhibit F. Operator shall either (1) enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, such that the Subprocessors agree to protect Data in a manner the same as or better than as provided pursuant to the terms of this DPA, or (2) indemnify and hold harmless the LEA, its officers, agents, and employees from any and all claims, losses, suits, or liability including attorneys' fees for damages or costs resulting from the acts or omissions of its Subprocessors. Operator shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this DPA. Supbrocessors shall agree to the provisions of the DPA regarding governing law, venue, and jurisdition.

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With State and Federal Law**. LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, Texas Education Code Chapter 32, and all other Texas privacy statutes cited in this DPA as these laws and regulations apply to the contracted services. The LEA shall not be required to provide Data in violation of applicable laws. Operator may not require LEA or users to waive rights under applicable laws in connection with use of the Services.

2. **Consider Operator as School Official.** The Parties agree that Operator is a "school official" under FERPA and has a legitimate educational interest in personally identifiable information from education records. For purposes of the Service Agreement and this DPA, Operator: (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from education records

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

4. **Unauthorized Access Notification**. LEA shall notify Operator promptly of any known unauthorized access. LEA will assist Operator in any efforts by Operator to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF OPERATOR

1. **Privacy Compliance**. Operator may receive Personally Identifiable Information ("PII") from the District in the course of fulfilling its duties and obligations under the Service Agreement. The Operator shall comply with all applicable State and Federal laws and regulations pertaining to data privacy and security including FERPA, COPPA, PPRA, Texas Education Code Chapter 32, and all other Texas privacy statutes cited in this DPA.

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

3. **De-identified Information**. De-identified Information may be used by the Operator only for the purposes of development, product improvement, to demonstrate or market product effectiveness, or research as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Operator agrees not to attempt to re-identify De-identified Information and not to transfer De-identified Information to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to LEA who has provided prior written consent for such transfer. Operator shall not copy, reproduce or transmit any De-identified Information or other Data obtained under the Service Agreement except as necessary to fulfill the Service Agreement.

4. **Access To, Return, and Disposition of Data**. Upon written request of LEA, Operator shall dispose of or delete all Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, and transfer said data to LEA or LEA's designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Operator acknowledges LEA's obligations regarding retention of governmental data, and shall not destroy Data except as permitted by LEA. Nothing in the Service Agreement shall authorize Operator to maintain Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Data; (2) Data Destruction; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Operator shall provide written notification to LEA when the Data has been disposed of.

The duty to dispose of Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Data" FORM, a sample of this form is attached on Exhibit "D"). Upon receipt of a request from the LEA, the Operator will immediately provide the LEA with any specified portion of the Data within five (5) business days of receipt of said request.

5. **Targeted Advertising Prohibition**. Operator is prohibited from using or selling Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Operator; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Operator from generating legitimate personalized learning recommendations.

6. **Access to Data**. Operator shall make Data in the possession of the Operator available tothe LEA within five (5) business days of a request by the LEA.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Operator agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Operator are set forth below. Operator shall further detail its security programs and measures in Exhibit F. These measures shall include, but are not limited to:

    a. **Passwords and Employee Access**. Operator shall secure usernames, passwords, and any other means of gaining access to the Services or to Data, at a level consistent with an industry standard agreed upon by LEA (e.g. suggested by Article 4.3 of NIST 800-63-3). Operator shall only provide access to Data to employees or subprocessors that are performing the Services. Employees with access to Data shall have signed confidentiality agreements regarding said Data. All employees with access to Data shall pass criminal background checks.

    b. **Security Protocols**. Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Operator shall maintain all data obtained or generated pursuant to the Service Agreement in a secure computer environment.

    c. **Employee Training**. The Operator shall provide periodic security training to those of its employees who operate or have access to the system.

    d. **Security Technology**. When the Services are accessed using a supported web browser, Secure Socket Layer ("SSL") or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Operator shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.

    e. **Security Contact.** Operator shall provide the name and contact information of Operator's Security Contact on Exhibit F. The LEA may direct security concerns or questions to the Security Contact.

    f. **Periodic Risk Assessment.** Operator shall conduct periodic isk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. Upon request, Operator will provide the LEA an executive summary of the risk assessment or equivalent report and confirmation of remediation.

g. **Backups.** Operator agrees to maintain backup copies, backed up at least daily, of Data in case of Operator's system failure or any other unforeseen event resulting in loss of any portion of Data.

h. **Audits.** Within 30 days of receiving **a** request from the LEA, and not to exceed one request per year, the LEA may audit the measures outlined in the DPA. The Operator will cooperate fully with the LEA and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Operator and/or delivery of Services to students and/or LEA, and shall provide full access to the Operator's facilities, staff, agents and LEA's Data and all records pertaining to the Operator, LEA and delivery of Services to the Operator. Failure to cooperate shall be deemed a material breach of the DPA. The LEA may request an additional audit if a material concern is identified.

i. **Incident Response.** Operator shall 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 any portion of Data, including PII, and agrees to provide LEA, upon request, an executive summary of the written incident response plan.

2. **Data Breach**. When Operator reasonably suspects and/or becomes aware of an unauthorized disclosure or security breach concerning any Data covered by this Agreement, Operator shall notify the District within 24 hours. The Operator shall take immediate steps to limit and mitigate the damage of such security breach to the greatest extent possible. If the incident involves criminal intent, then the Operator will follow direction from the Law Enforcement Agencies involved in the case.

a. The security breach notification to the LEA shall be written in plain language, and address the following

1. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
2. A description of the circumstances surrounding the disclosure or breach, including the actual or estimated, time and date of the breach, and Whether the notification was delayed as a result of a law enforcement investigation.

b. Operator agrees to adhere to all requirements in applicable state and federal law with respect to a Data breach or disclosure, including any required responsibilities and procedures for notification or mitigation

c. In the event of a breach or unauthorized disclosure, the Operator shall cooperate fully with the LEA, including, but not limited to providing appropriate notification to individuals impacted by the breach or disclosure. Operator will reimburse the LEA in full for all costs incurred by the LEA in investigation and remediation of any Security Breach caused in whole or in part by Operator or Operator's subprocessors, including but not limited to costs of providing notification and providing one year's credit monitoring to affected individuals if PII exposed during the breach could be used to commit financial identity theft.

d. The LEA may immediately terminate the Service Agreement if the LEA determines the Operator has breached a material term of this DPA.

e. The Operator's obligations under Section 7 shall survive termination of this DPA and Service Agreement until all Data has been returned and/or Securely Destroyed.

ARTICLE VI- GENERAL OFFER OF PRIVACYTERMS

1. **General Offer of Privacy Terms.** Operator may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached as Exhibit E), be bound by the terms of this DPA to any other LEA who signs the acceptance in said Exhibit.

ARTICLE VII: MISCELLANEOUS

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

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

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Operator shall dispose of all of LEA's Data pursuant to Article IV, section 5.

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

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives before: The designated representative for the Operator for this Agreement is:

First Name:	Daniel	[Box 7]
Last Name:	Pratte	[Box 8]
Operator's Company Name:	Labster Inc.	[Box 9]
Title of Representative:	High School Sales Manager	[Box 10]

The designated representative for the LEA for this Agreement is:

First Name:	Kyle	[Box 11]
Last Name:	Jones	[Box 12]
LEA's Name:	Lackland ISD	[Box 13]
Title of Representative:	Director of Technology	[Box 14]

6. **Entire Agreement**. This DPA constitutes the entire agreement of the parties relating to the subject matter and supersedes all prior communications, representations, or agreements, oral or written, by the Parties. 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.

7. **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.

8. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF TEXAS, 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 IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority**. Operator represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Data and portion thereof is stored, maintained or used in any way.

10. **Waiver**. Waiver by any party to this DPA of any breach of any provision of this DPA or warranty of representation set forth herein shall not be construed as a waiver of any subsequent breach of the same or any other provision. The failure to exercise any right under this DPA shall not operate as a waiver of such right. All rights and remedies provided for in this DPA are cumulative. Nothing in this DPA shall be construed as a waiver or relinquishment of any governmental immunities or defenses on behalf of the LEA, its trustees, officers, employees, and agents as a result of the execution of this DPA or performance of the functions or obligations described herein.

11. **Assignment**. The Parties may not assign their rights, duties, or obligations under this DPA, either in whole or in part, without the prior written consent of the other Party except that either party may assign any of its rights and obligations under this DPA without consent in connection with any merger (including without limitation by operation of law), consolidation, reorganization, or sale of all or substantially all of its related assets or similar transaction. This DPA inures to the benefit of and shall be binding on the Parties' permitted assignees, transferees and successors.

[*Signature Page Follows*]

IN WITNESS WHEREOF, the parties have executed this DATA PRIVACY AGREEMENT FOR TEXAS K-12 INSTITUTIONS as of the last day noted below.

Operator's Representative:

BY: Daniel Pratte [Box 15] Date: 12 / 10 / 2020 [Box 16]

Printed Name: Daniel Pratte [Box 17] Title/Position: High School Sales Manager [Box 18]

Address for Notice Purposes: 561 Windsor Street, B302 Somerville, MA 02143 [Box 19]

LEA's Representative

BY: Burnie Roper [Box 20] Date: 2-23-2021 [Box 21]

Printed Name: Dr. Burnie Roper [Box 22] Title/Position: Superintendent [Box 23]

Address for Notice Purposes: 2460 Kenly Ave, Building 8265 [Box 24]

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

Description : [Box 25]

See Labster Sole Source Letter.

LABSTER

To Whom It May Concern,

This letter is to inform you that the full function and capabilities of Labster's tailor-made and off-the-shelf virtual laboratory simulations are available only from Labster ApS. There is no equivalent product on the market available from another organization. Labster's simulation platform and all off-the-shelf virtual labs are owned fully by Labster ApS, including all intellectual property.

The Labster system is the only solution that can support integrated learning to utilize laboratory simulations, create immersive 3D virtual laboratories, with a menu of laboratories available for immediate use and develop bespoke laboratory simulations designed specifically for courses at University of Westminster based on case stories inspired by research at University of Westminster.

Labster is a laboratory simulation accessible directly in the web-browser where students can engage with life science experiments. All Labster's virtual labs are based on principles described in an article recently published in Nature Biotechnology where learning effectiveness and motivation level was assessed for several Labster labs.

Labster's tailor-made and off-the-shelf labs contain the following elements:

- 3D introductory scenes
- Storyboard and content, including in-lab text and quiz questions
- Laboratory 3D design
- 3D modeling and programming of 3D objects
- Lab workflow and interactivity
- Interactive 3D animations depicting what happens at a microscopic level
- Mathematical simulations and data export functions
- Theoretical section content
- Analytics dashboard for monitoring student performance
- A platform based on Open EdX

Sincerely,

EXHIBIT " B"

SCHEDULE OF DATA

Instructions: Operator should identify if LEA data is collected to provide the described services. If LEA data is collected to provide the described services, check the boxes indicating the data type collected. If there is data collected that is not listed, use the "Other" category to list the data collected.

☐ We do not collect LEA Data to provide the described services.

☒ We do collect LEA Data to provide the described services.

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	☐
	Other application technology meta data-Please specify:	☐
Application Use Statistics	Meta data on user interaction with application- Please specify:	☑
Assessment	Standardized test scores	☐
	Observation data	☐
	Other assessment data-Please specify: Multiple Choice Quiz Questions	☑
Attendance	Student school (daily) attendance data	☐
	Student class attendance data	☐
Communications	Online communications that are captured (emails, blog entries)	☐
Conduct	Conduct or behavioral data	☐
	Date of Birth	☐

	Demographics	Place of Birth	☐
		Gender	☐
		Ethnicity or race	☐
		Language information (native, preferred or primary language spoken by student)	☐
		Other demographic information-Please specify:	☐
	Enrollment	Student school enrollment	☐
		Student grade level	☐
		Homeroom	☐
		Guidance counselor	☐
		Specific curriculum programs	☐
		Year of graduation	☐
		Other enrollment information-Please specify:	☐
	Parent/Guardian Contact Information	Address	☐
		Email	☐
		Phone	☐
	Parent/Guardian ID	Parent ID number (created to link parents to students)	☐
	Parent/Guardian Name	First and/or Last	☐
	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:	☐

Category of Data	Elements	Check if used by your system
Student Contact Information	Address	☐
	Email	☑
	Phone	☐
Student Identifiers	Local (School district) ID number	☐
	State ID number	☐
	Vendor/App assigned student ID number	☐
	Student app username	☐
	Student app passwords	☐
Student Name	First and/or Last	☑
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:	☐
	Student bus assignment	☐
	Student pick up and/or drop off location	☐

	Transportation	Student bus card ID number	☐
		Other transportation data -Please specify:	☐
	Other	Please list each additional data element used, stored or collected through the services defined in Exhibit A	☐

EXHIBIT "C"

DEFINITIONS

HB 2087: The statutory designation for what is now Texas Education Code Chapter 32 relating to pupil records.

Data: Data shall include, but is not limited to, the following: student data, educational records, employee data, metadata, user content, course content, materials, and any and all data and information that the District (or any authorized end user(s)) uploads or enters through their use of the product. Data also specifically includes all personally identifiable information in education records, directory data, and other non-public information for the purposes of Texas and Federal laws and regulations. Data as specified in Exhibit B is confirmed to be collected or processed by the Operator pursuant to the Services. Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Operator's services.

De-Identified Information (DII): De-Identified Information is Data subjected to a process by which any Personally Identifiable Information ("PII") is removed or obscured in a way that eliminates the risk of disclosure of the identity of the individual or information about them, and cannot be reasonably re-identified.

Data Destruction: Provider shall certify to the District in writing that all copies of the Data stored in any manner by Provider have been returned to the District and permanently erased or destroyed using industry best practices to assure complete and permanent erasure or destruction. These industry best practices include, but are not limited to, ensuring that all files are completely overwritten and are unrecoverable. Industry best practices do not include simple file deletions or media high level formatting operations.

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

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, Data, metadata, and user or pupil-generated content obtained by reason of the use of Operator's software, website, service, or app, including mobile apps, whether gathered by Operator or provided by LEA or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Data.

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

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

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Operator, who Operator uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

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

Texas Student Privacy Alliance: The Texas Student Privacy Alliance (TXSPA) is a collaborative group of Texas school districts that share common concerns around student privacy. The goal of the TXSPA is to set standards of both practice and expectations around student privacy such that all parties involved have a common understanding of expectations. The Texas K-12 CTO Council is the organization that sponsors TXSPA and the TXSPA is the Texas affiliate of the National Student Privacy Consortium.

EXHIBIT "D"

SAMPLE REQUEST FOR RETURN OR DELETION OF DATA

Instructions: This Exhibit is optional and provided as a sample ONLY. It is intended to provide a LEA an example of what could be used to request a return or deletion of data.

_____ directs Labster Inc. to
LEA OPERATOR

dispose of data obtained by Operator pursuant to the terms of the Service Agreement between return LEA and Operator. The terms of the Disposition are set forth below:

1. Extent of Return or Disposition

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

☑ Return or Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Return or Disposition

☑ Disposition shall be by destruction or deletion of data.

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

3. Timing of Return or Disposition

Data shall be returned or disposed of by the following date:

☑ As soon as commercially practicable

☐ By the following agreed upon date:

4. Signatures

Authorized Representative of LEA	Date:

5. Verification of Disposition of Data

Daniel Pratte	12 / 10 / 2020
Authorized Representative of Operator	Date:

EXHIBIT " E"

GENERAL OFFER OF PRIVACY TERMS

Instructions: This is an optional Exhibit in which the Operator may, by signing this Exhibit, be bound by the terms of this DPA to any other Subscribing LEAs who sign the acceptance in said Exhibit. The originating LEA SHOULD NOT sign this Exhibit, but should make Exhibit E, if signed by an Operator, readily available to other Texas K-12 institutions through the TXSPA web portal. Should a Subscribing LEA, after signing a separate Service Agreement with Operator, want to accept the General Offer of Terms, the Subscribing LEA should counter-sign the Exhibit E and notify the Operator that the General Offer of Terms have been accepted by a Subscribing LEA.

1. Offer of Terms

Operator offers the same privacy protections found in this DPA between it and Lackland Independent School District and which is dated [12/10/20] to any other LEA ("Subscribing LEA") who accepts this General Offer through its signature below. This General Offer shall extend only to privacy protections and Operator's signature shall not necessarily bind Operator to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Operator and the other LEA may also agree to change the data provided by LEA to the Operator to suit the unique needs of the LEA. The Operator may withdraw the General Offer in the event of:

(1) a material change in the applicable privacy statutes;
(2) a material change in the services and products listed in the Originating Service Agreement;
(3) the expiration of three years after the date of Operator's signature to this Form.

Operator shall notify the Texas Student Privacy Alliance (TXSPA) in the event of any withdrawal so that this information may be may be transmitted to the Alliance's users.

Operator's Representative:

BY: Daniel Pratte Date: 12 / 10 / 2020

Printed Name: Daniel Pratte Title/Position: High School Sales Manager

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Operator, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and Operator shall therefore be bound by the same terms of this DPA. The Subscribing LEA, also by its signature below, agrees to notify Operator that it has accepted this General Offer, and that such General Offer is not effective until Operator has received said notification.

Subscribing LEA's Representative:

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

EXHIBIT "F"

DATA SECURITY

1. **Operator's Security Contact Information:**

Quyen McCarthy [Box 26]

Named Security Contact

quyen@labster.com [Box 27]

Email of Security Contact

6177181223 [Box 28]

Phone Number of Security Contact

2. **List of Operator's Subprocessors:**

See Labster Security Policies on next pages. [Box 29]

3. **Additional Data Security Measures:**

See Labster Security Policies on next pages. [Box 30]

Labster

March 2019

Security Program Overview

Whole organization security policies, procedures and documents. Special attention: persons with access to FERPA (students data) or PCI (credit cards) regulated data.

- Disk encryption
- GPG keys
- Labster Security Policies
    - Acceptable Encryption Policy
    - Acceptable Use Policy
    - Antivirus and Firewall Policy
    - Disaster Recovery Plan (lead links only)
    - Email Policy
    - Messenger Policy
    - Password Construction Guidelines
    - Password Protection Policy
    - Secure Software Development Life Cycle
- Maintaining Google account secure way
- Planning security enhancements
- Disaster Reaction Plans
    - Device Theft Reaction Plan

Labster

March 2019

DevOps disaster recovery plans

Computer Emergency Response Plan

Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?

When

There are certain situations when DevOps team members should be contacted on an emergency. Emergencies are usually posted in #escalation-team Slack channel. Typical situations:

- One of customer-facing systems are down, which cause service interruptions.
- Other (possible security problems, on #escalation-team members discretion)

How

1. Post direct message with @devops mention in #devops channel
2. (if previous step fails) Post direct message to DevOps Alert Tzar
3. (if previous step fails) Try to call via Slack. Try to call via Hangouts.
4. (if previous step fails) Direct phone call to one of DevOps team members (all phone numbers are listed in Slack profiles)

Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.

The discussion about any ongoing problems should be started in #escalation-team. Team members then decide whom to contact and when.

Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.

Data is stored on RDS and EC2 servers.

- API:
    - SimLic:
        - EC2 custom PostgreSQL instance.
    - Central region:
        - EC2 custom PostgreSQL instance in US
    - UK region:
        - EC2 custom PostgreSQL instance in UK
- Theory:

- MySQL RDS in US

All data is being stored with Amazon AWS. In case of account loss (termination, deletion, compromise) backup of backup also stored on Google compute engine, so we can restore all services from there.

Criticality of Service List: List all the services provided and their order of importance. It also explains the order of recovery in both short-term and long-term time frames.

Front Line Sytems (interactions with end users)

1. API2 region (note, regional services can survive some time even without simlic database functioning)
    1. central region
    2. UK- region
2. Theory

Infrastructure critical systems

1. Simlic (Simulations and Licenses)
2. SalesForce

Other systems

1. Sandboxes (some are accessed by integrators and collaborators)
2. Infrastructure services:
    1. Bamboo main server and workers
    2. Image Manager
    3. Release Manager
    4. Sentry

Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and

how often the backup is done. It should also describe how that data could be recovered.

- Central region data is backed up encrypted to Amazon S3 bucket: "labster-edx-db-backups".
- Regional data is backed up to Amazon S3 buckets named as: ""labster-edx-db-backups-<REGION>" - where <REGION> should be replaced with the 2 letter ISO code of country, where region is located.

In case if Amazon AWS backups are not accessible, BoB (Backup of Backups) is available.

Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.

Labster uses cloud deployment. Following is an action plan to replace any of the cloud components.

API2 regional databases

In case of any of regional databases failure, there is no replication enabled (at the moment). As a result, the data loss could be up to 24hrs in case if EC2 database instance is lost.
To restore the regional database following should be done:

- Create new EC2 regional database using Ansible scripts (FIXME *provide the command*)
- Enable replication
- Upload data from backup

Due to replication, if there was an event of data removal from SimLic, there could be a case when the database won't import. Ask @web-devs team for support, but the generic way to resolve it is:

1. Unpack file using pg_restore utility to plain SQL
2. Look at file using 'less' and then '-N' to see line numbers
3. Split file using 'split -l' to the part without constraints
4. Import first part.

5. Apply those constrains which apply. Skip those, which done, ask @web-devs to fix issues.

API2 simlic

In case of simlic database failure there might not be the need for immediate restoration, as this service is not customer facing. It could be wise idea to plan the replacement on closest weekend and then:

1. Notify users about maintenance works on weekend.
2. Create new EC2 instance and restore Simlic database from backup.
3. For every regional service:
    1. Stop backend instances
    2. Backup regional tables data
    3. Clean up the database
    4. Setup replication from new simlic database
    5. Upload regional data back (from step 2)

Theory

Theory service has standard backup, stored on S3. In case of theory RDS failure, there are also RDS snapshots, so:

1. Try to restore from Snapshot
2. (if step above failed) Try to restore from S3 backup
3. (if step above failed) Get BoB copy

Other ’infrastructure’ servers

All servers in the Labster ’infra’ cluster has their own backups, stored in same S3 bucket ("labster-edx-db-backups")

Sandboxes

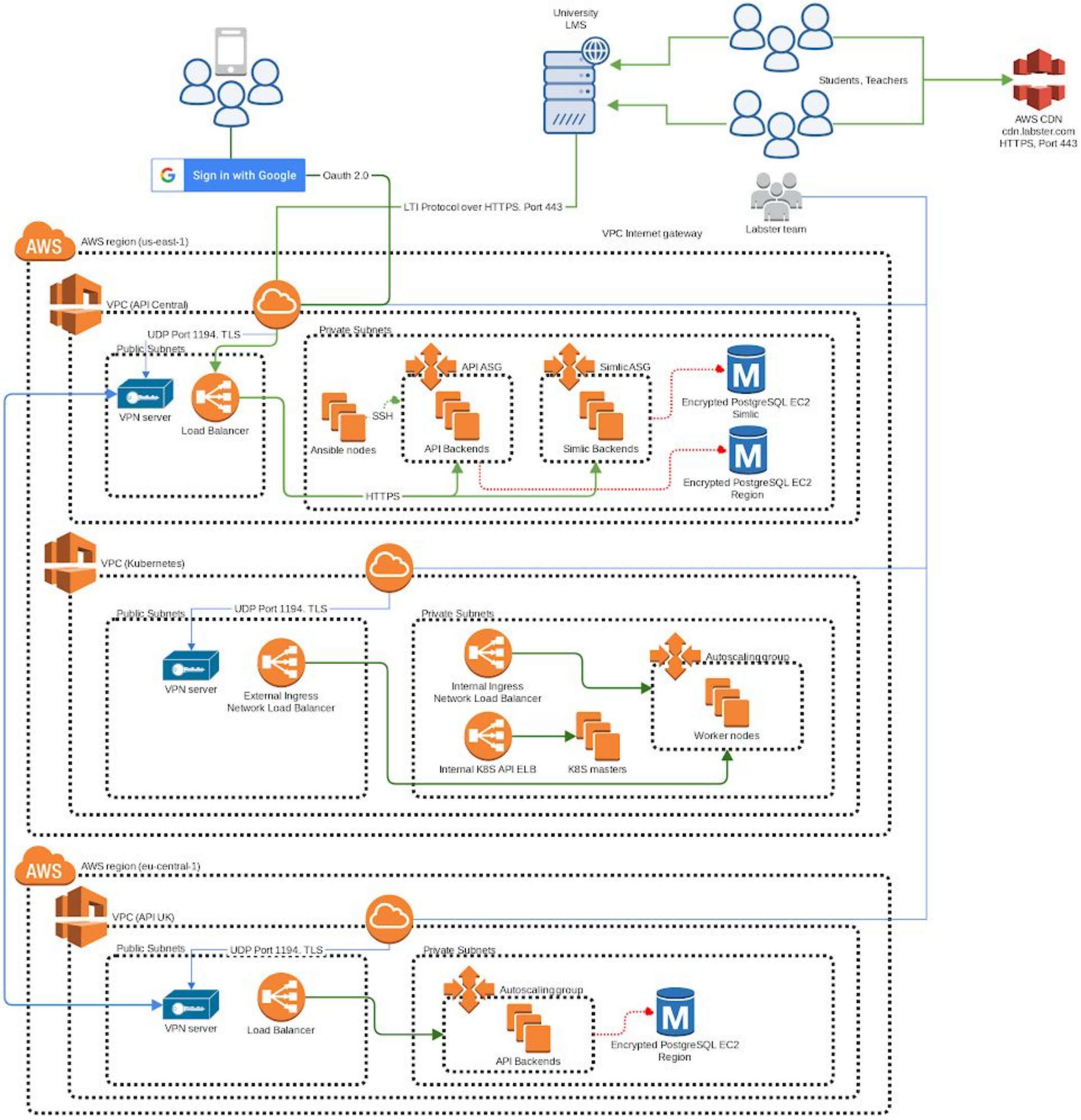
Sandboxes do not have default backups. Sandbox owners can decide to do sandbox backups on their own decision, in this case, if sandbox hardware is failed, the old sandbox should be removed (using Slack or @devops help) and then new one created, with same name, and database uploaded back.

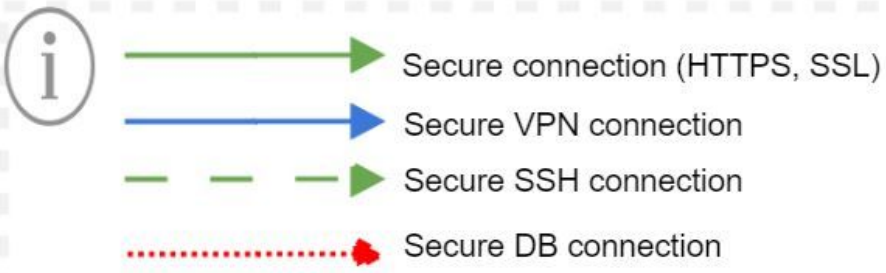
Mass Media Management: Who is in charge of giving information to the mass media?

When some event of failure, data breach, hacking etc happens, this information should be posted in Labster Slack in:

- #customer-success
- #escalation-team

Architecture diagram (API, Theory, Deployment nodes)





Core concepts

* Database connections are encrypted using SSL protocol
* Force HTTP requests redirect to HTTPS
* Customer authenticate each server by SSL certificate which signed by known certificate authority
* API authorization by token (LTI protocol)

Terms

Theory - Wiki style service, it contains theory for simulations and requires does not require login to access it.

Basic LTI uses the OAuth protocol (http://www.oauth.net) to secure its message interactions between the LTI Consumer and LTI Tool Provider (TP). OAuth requires a key and shared secret to sign messages. The key is transmitted with each message, as well as an OAuth-generated signature based on the key. The TP looks up the secret based on the provided key and re-computes the signature and compares the recomputed signature with the transmitted signature to verify the sender's credentials.

https://www.imsglobal.org/specs/ltiv1p0/implementation-guide

Labster team manage servers using SSH protocol over secure VPN connection. Port 22 for SSH is opened only for VPN access server and filtered for other sources.

API and Theory backends placed in different AWS Availability zones inside region US East (N. Virginia)

Labster

March 2019

Secure Software Development Life Cycle Overview

Labster uses Holacracy, OKR and Agile (Scrum, Kanban) as frameworks of organisational and development life cycles.
We have the following development agile teams in the organisation.

Team	Agile type	Purpose
Unity	Scrum	Developers of actual simulations
Web	Scrum/Kanban	Developers/devops of Labster web services

Development phases

We have following development phases:

1. Requirements
2. Design
3. Development & testing
4. Maintenance
5. Disposal, if required by clients

Roles and responsibilities

Role	Responsibility
Unity developer	Writing code and documentation that adheres to the acceptance criteria, maintaining and increasing test code coverage
Scrum master	Coaching circle members on Agile/Lean principles and practices as-needed or as-requested Defining and implementing issue tracking (i.e. epics, features, and bugs), and estimating workflow, processes, and policies Defining meeting processes and frequency, and facilitating meetings not required by the Holacracy Constitution Ensuring good process of estimating and communicating deadlines within development team and stakeholders
Product owner	Prioritizing and sequencing backlog items Defining the user stories and their acceptance criteria Approving working product deliverables
Devops	Maintaining and monitoring all web servers

	Deploying and documenting deployment process, access information and configuration Securing server setup Backuping of all databases regularly
Web developer & architects	Ensuring a scalable architecture among our services Accepting, rejecting and discussing changes to the web architecture Developing, documenting, securing and maintaining the backend and frontend Create security policy for development processes
QA	Creating test plan, testing, smoke testing, reporting, finding bugs Making sure all features meets product owner needs. Creating and maintaining Test Plan & Cases. Completing test result in Test Cases.
Security coordinator	Keep all source code and sensitive customer data highly protected on our servers and team members computers Getting password contract signatures from all team members Organising security training sessions for new team members

Development lifecycle security procedures

1. Requirements

During requirement phase, product owner of organisation prepares and prioritise list of features they want to be developed.
Every feature is considered to comply with existing security alignment of the platform and security standards of our clients.
Gathering security requirements and risk assessment is part of this phase.

2. **Design**
   During the design phase architects of the system provide the plan and architecture to implement feature to comply with all the security needs.
   Also they assess all 3rd party libraries used in the project to comply with the security needs.
   Security design and threat modelling is also part of this phase.

3. **Development & testing**
   Developers are ensured that security is handled correctly. QA perform checks of all features.
   1. Developers ensure that new code features and 3rd party applications do not introduce security issues
   2. Devops engineers ensure that changes to server environment do not introduce and lower security issues

3. Devops engineers ensure that server packages are up-do-date with all security patches
4. Devops engineers ensure that network configuration is secure
5. Code reviews are conducted regularly for every pull requested code by developers/devopses.
6. Architects and developers design new features with security in mind
7. Devops engineers ensure backups are in place
8. Developers aim for 95% test coverage
9. CI process is in place
10. Bug fixing policy in place: critical severity bugs are fixed during next 1-2 days, high severity bugs are fixed during current sprint, medium severity bugs are fixes during next sprint.

4. **Maintenance**
   Any issue or bug found in maintenance period is triaged and proper reaction is implemented. Critical and high priority bugs are fixed within current sprint.
   Medium and low priority bugs are within next sprints.
   Stress tests and security web scans are part of this phase.
   Incident reporting procedure is in place.
   Backup procedures are in place.

5. **Disposal**
   After disposal of service for a given client, all user information for the given client is cleaned up from the system and from backups.
   After deletion of information for the given client from backups, backups are archived and encrypted. Backups are digital.

Release procedures

New requirements are formulated and prioritised by product owners and are put to the product backlog.
Every two weeks next set of tasks is taken into development to the current scrum.
After feature is ready and tested in different environments, it is deployed to production.
Our scrums are two weeks long, so it is fairly short release cycle for new features.

Labster

March 2019

Acceptable Encryption Policy

1. Overview

See Purpose.

2. Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

3. Scope

This policy applies to all Labster employees.

4. Policy

4.1 Algorithm Requirements

1. Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.
2. Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.
3. Signature Algorithms

Algorithm	Key Length (min)	Additional Comment
ECDSA	P-256	Cisco Legal recommends RFC6090 compliance to avoid patent infringement.
RSA	2048	Must use a secure padding scheme. PKCS#7 padding scheme is recommended. Message hashing required.
LDWM	SHA256	Refer to LDWM Hash-based Signatures Draft

4.2 Hash Function Requirements

In general, Labster adheres to the NIST Policy on Hash Functions.

4.3 Key Agreement and Authentication

1. Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).
2. End points must be authenticated prior to the exchange or derivation of session keys.
3. Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.
4. All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.
5. All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

4.4 Key Generation

1. Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.
2. Key generation must be seeded from an industry standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

5. Policy Compliance

5.1 Compliance Measurement

The Labster Security coordinator will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Labster Security coordinator in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

National Institute of Standards and Technology (NIST) publication FIPS 140-2,
NIST Policy on Hash Functions

Acceptable Use Policy

1. Overview

Information security department intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Labster's established culture of openness, trust and integrity. Information security department is committed to protecting Labster's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, and file transfers, are the property of Labster. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Personal use that is opposing (inter-)national laws or are a threat to Labster's business, e.g. illegal file sharing, usage of torrent, access of pornographic, racist or any other type of harmful, malicious or deeply disrespectful content via Labster infrastructure is prohibited. Please review Human Resources policies for further details

Effective security is a team effort involving the participation and support of every Labster employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Labster. These rules are in place to protect the employee and Labster. Inappropriate use exposes Labster to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Labster business or interact with internal networks and business systems, whether owned or leased by Labster, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Labster and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Labster policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Labster, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Labster.

4. Policy

4.1 General Use and Ownership

4.1.1 Labster proprietary information stored on electronic and computing devices whether owned or leased by Labster, the employee or a third party, remains the sole property of Labster. You must ensure through legal or technical means that proprietary information is protected in accordance with the Password Protection Policy.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Labster proprietary information.

4.1.3 You may access, use or share Labster proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Any Limitations and Restrictions in acceptable use of Internet/Intranet/Extranet systems described in policies of your circle(s) that are conflicting with points of this policy needs to be clarified with your supervisor or manager to approve your planned actions.

4.1.5 For security and network maintenance purposes, authorized individuals within Labster may monitor equipment, systems and network traffic at any time.

4.1.6 Labster reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.1.7 If you discover any unauthorized external access of Labster infrastructure or any scenario described inside Disaster Recovery Plan (lead links only) you must report to IT Disaster Reaction Planner and follow the steps in its respective scenario reaction plan immediately.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the Password Protection Policy.

4.2.2 System level and user level passwords must comply with the Password Protection Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4 Postings by employees from a Labster email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Labster, unless posting is in the course of business duties.

4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Labster authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Labster-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Labster.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Labster or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server or an account for any purpose other than conducting Labster business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to the export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing the use of your account by others. This includes family and other household members when work is being done at home.
7. Using a Labster computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any Labster account.
9. Making statements about warranty such as compensation or coverage of damage while using Labster tools and services, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service,

and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Introducing honeypots, honeynets, or similar technology on the Labster network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, Labster employees to parties outside Labster.

4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the Labster Security coordinator.
1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Labster's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Labster or connected via Labster's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.3 Blogging and Social Media

1. Blogging by employees, whether using Labster’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Labster’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Labster’s policy, is not

detrimental to Labster’s best interests, and does not interfere with an employee's regular work duties. Blogging from Labster’s systems is also subject to monitoring.
2. Labster’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Labster's confidential or proprietary information, trade secrets or any other material covered by Labster’s Confidential Information policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Labster and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Labster’s Non-Discrimination and Anti-Harassment policy.
4. Employees may also not attribute personal statements, opinions or beliefs to Labster when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Labster. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Labster’s trademarks, logos and any other Labster intellectual property may also not be used in connection with any blogging activity

5. Policy Compliance

5.1 Compliance Measurement

The Labster Security coordinator will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Labster Security coordinator in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Labster

March 2019

Antivirus and Firewall Policy

Overview

Labster systems are under a constant risk of security breaches leading to theft, misuse, modification or deletion of Company and Customer information and Labster-owned or Labster-associated services. While the installation of trusted Antivirus and Firewall software will not cover every case of security hazard it is still considered secure for most common malware threats. Not having devices properly protected may lead to compromising, exploitation and damage of the whole Labster IT infrastructure.

Purpose

The purpose of this policy is to stipulate that anti-virus software and firewall must be installed by default on all Labster-accessing systems. Any exceptions need to be documented and justified by the system owner. Any device connecting to Labster-owned or Labster-associated services may be denied access if it is not running minimum anti-virus and firewall software.

Scope

All Labster employees, vendors, and agents operating on behalf of Labster and using Labster-built and managed systems (including servers, desktops, laptops and mobile devices). All devices connecting to Labster-owned or Labster-associated services. All third party built and hosted systems used by Labster.

Policy

Employee is required to protect Labster-accessing devices with trusted antivirus and firewall software. These software can be either the enabling of built-in software such as standard Windows 7, 8, 10 Network firewall, Virus and Spyware protection or the download of trusted Antivirus and Firewall software.
Employee is required to keep antivirus and firewall software up-to-date.
A regular (automated) update of the software is mandatory to ensure highest protection possible.
A regular machine scan for existing malware, viruses and other security hazards is advised.
Latest scans should not be older than 90 days.

Trusted Antivirus/Firewall Security software

Windows OS:

- Windows internal Virus protection + Windows internal Spyware and unwanted software protection + Windows internal Network firewall
- Norton Antivirus (Symantec)
- McAfee Antivirus
- Bitdefender
- Trend Micro
- AVG
- Avira Free Antivirus
- Zonealarm free (Firewall only)
- ...

Android OS:

- 360 Security - Antivirus Boost
- AndroHelm Mobile Security
- Avira Antivirus Security
- Antivirus and Mobile Security by TrustGo
- AVAST Mobile Security
- AVG Antivirus Security
- Bitdefender Antivirus Free
- Norton Antivirus and Security
- ...

Policy Compliance

Antivirus and firewall software on devices are installed, active and up-to-date.

Exceptions

Operating systems that don't naturally need or support antivirus or firewall software. Employees supervisor needs to be informed and confirm the use of unprotected devices and the non-observance of this policy in coordination with Labster Security Coordinator.

Non-Compliance

An employee found to have violated this policy which resulted into harm of Labster infrastructure, damage, information loss or similar may be subject to disciplinary action, up to and including termination of employment.

Labster

March 2019

Email Policy

1. Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

2. Purpose

The purpose of this email policy is to ensure the proper use of Labster email system and make users aware of what Labster deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within Labster Network.

3. Scope

This policy covers appropriate use of any email sent from a Labster email address and applies to all employees, vendors, and agents operating on behalf of Labster.

4. Policy

4.1 All use of email must be consistent with Labster policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

4.2 Labster email account should be used primarily for Labster business-related purposes; even though personal communication is encouraged by Labster, non-Labster related commercial uses such as the use of Labster email account for eBay/Amazon/Tokopedia/Facebook are prohibited.

4.3 All Labster data containing sensitive information (passwords, secure keys, customer data) should be transferred between employees using LastPass Sharing Center. If due to some reason LastPass can not be used (for example for server-side automated things), please consult Acceptable Encryption Policy and choose appropriate encryption standard (for example GPG is used now server-side to store encrypted backups).

4.4 Email should be retained only if it qualifies as a Labster business record. Email is a Labster business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

4.5 Email that is identified as a Labster business record shall be retained according to Labster Record Retention Schedule.

4.6 The Labster email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color,

disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Labster employee should report the matter to their supervisor immediately.

4.7 Users are prohibited from automatically forwarding Labster email to a third party email system (noted in 4.8 below) if forwarded information can be used against Labster. Individual messages which are forwarded by the user must not contain unprotected Labster confidential or above information.

4.8 Users are prohibited from using third-party email systems and storage servers such as Yahoo, and MSN Hotmail etc. to conduct Labster business, to create or memorialize any binding transactions, or to store or retain email on behalf of Labster. Such communications and transactions should be conducted through proper channels (e.g. LastPass, Labster Google accounts) using Labster-approved documentation.

4.9 Using a reasonable amount of Labster resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a Labster email account is prohibited.

4.10 Labster employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.

4.11 Labster may monitor messages without prior notice. Labster is not obliged to monitor email messages.

4.12. Users are allowed to use offline Email access clients such as Thunderbird, Outlook Express or any other. In such case the the local storage must be encrypted and the mail client software should not contain any known security flaws.

5. Policy Compliance

5.1 Compliance Measurement

The Labster Security team will verify compliance to this policy through various methods, including but not limited to, random walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Labster Security Coordinator in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

- Password Construction Guidelines
- Password Protection Policy
- Acceptable Encryption Policy

Labster

March 2019

Messenger Policy

1. Overview

To keep the information flow steady and project coordination on a transparent and informal level we are using third party instant messaging services, currently Slack. Although Slack claims that its service is secure and protected, broader incidents such as information leakage and information theft should always be considered.

2. Purpose

This policy is in place to raise awareness and suggests best practices for sensitive information sharing using messaging services.

3. Scope

This policy covers appropriate usage of any message sent with the official instant (group-) messaging service *Slack.* It applies to all employees, vendors and agents operating on behalf of Labster.

4. Policy

4.1 The accepted service for instant messaging on work related discussions is *Slack*.

4.2 Employees are allowed to use other third party messengers for *informal usage and coordination* if communication via *Slack* cannot be established between all parties and usage will not negatively affect work moral or coordination reach. (e.g. usage of WhatsApp group chat for informal non-work related discussions or coordination; Facebook group chat to coordinate weekly sports events)

4.3 Employees are prohibited to use other third party messengers for *work related communication* if it would expose sensitive information.

4.4 All use of instant messaging must be consistent with Labster policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

4.5 All Labster data containing sensitive information (passwords, secure keys, customer data) should be transferred between employees using LastPass Sharing Center. If due to some reason LastPass can not be used (for example for server-side automated things), please consult Acceptable Encryption Policy and choose appropriate encryption standard (for example GPG is used now server-side to store encrypted backups).

4.6 Labster employees shall have no expectation of privacy in anything they store, send or receive on the company's messaging system.

4.7 Labster may monitor messages without prior notice. Labster is not obliged to monitor messages.

5. Policy Compliance

5.1 Compliance Measurement

The Labster Security team will verify compliance to this policy through various methods, including but not limited to, random walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Labster Security Coordinator in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

Acceptable Encryption Policy
Password Protection Policy

Password Protection Policy

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Labster's resources. All users, including contractors and vendors with access to Labster systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Labster facility, has access to the Labster network, or stores any non-public Labster information.

4. Policy

4.1 Password Creation

1. All users are encouraged to use LastPass password generation facility. Please refer to Password Construction Guidelines for more information how to create secure passwords.
2. All user-level and system-level passwords must conform to the Password Construction Guidelines.
3. Users must not use the same password for Labster accounts as for other non-Labster access (for example, personal ISP account, option trading, benefits, and so on).
4. Where possible, users must not use the same password for various Labster access needs.
5. User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.

4.2 Password Protection

1. All passwords should be stored securely. It is highly advised to always use LastPass to store and share (where necessary) all passwords, passphrases and passcodes . If LastPass can not be used, Acceptable Encryption Policy for storing passwords must be followed.
2. Passwords must not be inserted into email messages, google docs/drive, attached files or other forms of electronic communication except LastPass sharing center.
3. Passwords must not be revealed over the phone to anyone.
4. Do not reveal a password on questionnaires or security forms.
5. Do not hint at the format of a password (for example, "my family name").
6. Do not share Labster passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
7. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
8. LastPass is integrated to most common browsers and provides the ability to securely remember passwords for sites. Using browsers internal "Remember Password" feature should be discouraged as many browsers do not store passwords securely.
9. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

4.3. Password sharing

1. Always choose to have several accounts for the same role or service over sharing passwords for single account when it is possible
2. Make sure to use secure method of sharing passwords, for example use LastPass sharing center or GPG encryption or equivalent secure channel (please refer to Acceptable Encryption Policy)

4.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

1. Applications must support authentication of individual users, not groups.
2. Applications must not store passwords in clear text or in any easily reversible form.
3. Applications must not transmit passwords in clear text over the network.
4. Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4.5 Use of Passwords and Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access. Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

```
The*?#>*@TrafficOnThe101Was*&#!#ThisMorning
```

All of the rules above that apply to passwords apply to passphrases.

Policy Compliance

5.1 Compliance Measurement

The Labster Security team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Labster Security Team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

Password Construction Guidelines

Password Construction Guidelines

Overview

Passwords are a critical component of information security. *Passwords* serve to protect user accounts; however, a poorly constructed P*assword* may result in the compromise of individual systems, data, or the network. This guideline provides best practices for creating secure *Passwords*.

Purpose

The purpose of this guidelines is to provide best practices for the created of strong *Passwords*.

Scope

This guideline applies to *Employees* as we defined them in Security Policies definitions section. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

Statement of Guidelines

Whenever possible, use LastPass to generate and store strong *Passwords*:

- https://lastpass.com/generatepassword.php

All *Passwords* should meet or exceed the following guidelines
Strong passwords have the following characteristics:

- Contain at least 12 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).

Poor, or weak, *Passwords* have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.

- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a *Passwords*. Either use LastPass to store all crypted geneted passwords or try to create *Passwords* that you can remember easily. One way to do this is create a *Password* based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the *Password* TmB1w2R! or another variation. (NOTE: Do not use either of these examples as *Passwords*!)

To test how good your *Password* is, you can use this online tool:

- https://www.grc.com/haystack.htm

Enter a similar *Passwords* with the same number of lowercase and uppercase letters, symbols, and numbers at https://www.grc.com/haystack.htm. (**Don’t enter your actual** *Password* on any webpage unless you’re logging into its associated account.) Under Time Required to Exhaustively Search this *Password's* Space, ensure that the Massive Cracking Array Scenario will take more than one year.

Passphrases

Passphrases generally are used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the *Passphrases* to unlock the private key, the user cannot gain access.

A *Passphrase* is similar to a *Password* in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong *Passphrases* should follow the general *Password* construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

Passcodes

Devices without Touch ID should use Passcodes as minimum protection.

Devices with Touch ID are known as sufficiently secure and do not require an additional Passcode. For Devices without this option use a complex Passcode that meets the other requirements in this list.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Processing User Data Documentation

Data Process Purpose	
For what purpose is the personal data processed?	Labster is an online educational tool for science students. Integrating Labster in Moodle, Canvas, Blackboard etc. allows students and instructors to access Labster simulations via the institution's virtual learning environment/learning management system (VLE/LMS) directly. Labster Support team has access to the Dashboard displaying students email addresses and their scores obtained within Labster simulations. This is needed in order to provide support to individual students or course instructor upon request. Score data is kept for internal analytics, but the obfuscation removes any chance of identifying a personal user or individual in compliance with known security norms. We do not sell, trade, or rent users personal identification information to others. Labster ApS may collect and use Users personal information for the following purposes: 1. *To improve customer service* Information you provide helps us respond to your customer service requests and support needs more efficiently. 2. *To personalize user experience* We may use information in the aggregate to understand how our Users as a group use the services and resources provided on our Site. 3. *To improve our Site* We may use feedback you provide to improve our products and services. 4. *To process payments* We may use the information Users provide about themselves when placing an order only to provide service to that order. We do not share this information with outside parties except to the extent necessary to provide the service. 5. *To run a promotion, contest, survey or other Site feature* To send Users information they agreed to receive about topics we think will be of interest to them. 6. *To send periodic emails* We may use the email address to send User information and updates pertaining to their order. It may also be used to respond to their inquiries, questions, and/or other requests. If User decides to opt-in to our mailing list, they will receive emails that may include company news, updates, related product or service information, etc. If at any time the User would like to unsubscribe from receiving future emails, we include detailed unsubscribe instructions at the bottom of each email or User may contact us via our Site. 7. *To conduct scientific research* We may use the information to conduct scientific research that may lead to publications in scientific journals and conferences.
Types of Data Processed and Nature of processing	
What is the nature of processing?	The LMS (Moodle, Canvas, Blackboard, etc.) connects to the specific Labster learning simulations on the Server API using HTTPS and sends student id, email and name. Nothing else is transmitted from the LMS to Server API, and only HTTPS connections are accepted. We rely on Amazon Web Servers (AWS) as our deployment architecture, all data in transfer is encrypted even on the local network and all personal data is situated on encrypted partitions. * All databases and database backups are stored using encrypted RDS instances. * All developers that have access to production and backup databases never use databases with sensitive information for local development. * All local hard drives used by developers are although still also encrypted. We have a main staging server (a copy of the production environment) as well as individual sandbox servers. All servers are hosted on Amazon Web Services in similar environments and are completely independent, to ensure no tests affect the production environment. This ensures that any tests performed on sandbox or staging servers will mimic the production environment and ensure minimum risk of deployment-related problems.

What type of personal data is being processed?	Labster takes responsibility for secure transfer, storage and maintaining access policies to the customer's information assets, including personal information. All information is stored either on encrypted RDS or EC2 encrypted partition. The data is compiled of the following: *Anonymous user IDs from the LMS (used in LTI Oauth2 based authorization process) * Personal student information: (a) Email address, First and Last name. * Grades data * Simulation events data (to resume/continue of current simulation, and for performance/ statistic Labster has data obfuscation by request. Email Addresses, First Name, Last Name are obfuscated. Score data is kept for internal analytics, but the obfuscation removes any chance of identifying a personal user or individual in compliance with known security norms. All sensitive data is encrypted as it travels over each network connection. All connections to Labster services use SSL as transport layer encryption. Our simulations and server setup furthermore enforce the use of HTTPS connections and will prevent any use of insecure HTTP connections by preventing the connection attempt. Furthermore, all internal connections within Labster servers to Amazon RDS databases as well as between nodes within the VPC, are encrypted using SSL, which effectively means 100% of connections are safe.
What category of data is being processed?	Labster is processing only personal data. Labster does not deal with any kind of sensitive information such as race, ethnic origin, political, religious or philosophical beliefs or union affiliation, as well as the treatment of genetic data, biometric data for the purpose of unambiguously identifying a natural person, health information or information about a sexual personality or sexual orientation.
Use of the service by minors?	Individuals under the age of 18 may not use the Service unless their Entity enters into an agreement with Labster that allows such individuals to use the Service. In the event that you provide a minor with access to use the Service, you hereby agree to this Agreement on behalf of yourself and such minor, and you understand and agree that you will be responsible for all uses of the Service by the minor you provide access to use the Service whether or not such uses were authorized by you.
Where do the personal data come from?	Personal data comes from data subjects themselves. Students enter the requested data by themselves.
On what legal ground are the personal data processed?	Personal data is processed according to the contract that Labster and all of its customers have been agreed to sign.
Is processing of the personal data necessary for the purpose?	Yes. Labster Support team has access to the Dashboard displaying students email addresses and their scores obtained within Labster simulations. This is needed in order to provide support to individual students or course instructor upon request.
What is the duration of the data processing?	Processing shall not be time-limited and shall be performed until this Data Processing Agreement is terminated or cancelled by one of the Parties.
Access Management	

<table>
<tr><td>Who has access to personal data?</td><td>Support team members have access due to the nature of their work based on the below matrix. Other team members never have access in full only by web panel where individual requests can be seen. This access is granted by the security team. s. Current AWS permission matrix:

<table>
<tr><th>GROUP NAME</th><th>PERMISSION</th><th>PURPOSE</th></tr>
<tr><td>Billing</td><td>Billing full access</td><td>Billing details for finance dept</td></tr>
<tr><td>Content</td><td>AmazonS3FullAccess
CloudFrontFullAccess</td><td>Full access to S3 and CloudFront for content writers</td></tr>
<tr><td>Devops</td><td>AdministratorAccess</td><td>Full access to all AWS infrastructure and services for DevOps team</td></tr>
<tr><td>Management</td><td>AdministratorAccess</td><td>Full access to all AWS infrastructure and services for head management</td></tr>
<tr><td>Unity</td><td>AmazonS3FullAccess
CloudFrontFullAccess</td><td>Full access to S3 and CloudFront for Unity developers</td></tr>
<tr><td>Web</td><td>AmazonS3FullAccess
CloudFrontFullAccess</td><td>Full access to S3 and CloudFront for Web developers</td></tr>
</table></td></tr>
<tr><td>Who manages the accounts? Automated system or process administrator?</td><td>Accounts are managed in your organization's LMS system, Labster does not manage the accounts. Accounts information (students, teachers) is being sent over LTI protocol (secure) to Labster API.</td></tr>
<tr><td>Describe the procedures used to authenticate user identity, authorize user access, and terminate users when they leave or change positions</td><td>• Central database access privileges revoked by Labster security officer
* Company access revoked from Google For Work
* AWS access keys are deleted by DevOps team</td></tr>
<tr><td>What will be the authorization process for granting user accesses and privileges? How will users be enrolled into the system?</td><td>Enrollment is done on the LMS. Labster API will authorize users to use certain resources based on License code for the selected courses and Consumer keys configured in LMS.</td></tr>
<tr><td>How do you ensure that there will be no internal unauthorized access to personal data?</td><td>All data is transferred using TLS. Labster API will refuse to send/receive data for non-validating certificates. New Relic and DataDog monitoring can show unusual network/CPU activities usually associated with compromises;

We are using Papertrail to collect all logs and OSSEC to watch the potential security threats. OSSEC watches everything and actively monitors all aspects of the Unix system activity with file integrity monitoring, log monitoring, rootcheck and process monitoring.

We furthermore use push notifications sent through New Relic and Datadog to inform the entire team of any server issues to ensure fast reaction time.

• All events are logged to local syslog
• All syslog events are security transferred to Papertrail cloud service

Only authorized team members are granted access to Papertrail service. Labster software does not authenticate any users: only authorization is done via OAuth2 based LTI protocol.

In addition to this, there is a procedure for access revocation.</td></tr>
<tr><td>Who is responsible for data protection compliance? What are their responsibilities?</td><td>Labster Security Coordinator, Web Security Officer, DevOps Security officer, IT Disaster Reaction Planner, Data Wrangler are defined, documented and assigned roles within Labster connected to security coordination and work. All DevOps team members have the necessary training in operational security. All new code is being double checked and signed by at least 2 persons (Pull Request Reviewers). The web team has a security officer who is responsible for regular code reviews.</td></tr>
<tr><td>Use of Sub-processors</td><td></td></tr>
</table>

What are the terms under which sub-processors are used?	The Data Processor has the Data Controller's general consent for the engagement of sub-processors. We rely on Amazon Web Servers (AWS) as our deployment architecture, all data in transfer is encrypted even on the local network and all personal data is situated on encrypted partitions. Labster shall, however, inform the Data Controller of any planned changes with regard to additions to or replacement of other data processors and thereby give the Data Controller the opportunity to object to such changes. If the Data Controller should object to the changes, the Data Controller shall notify Labster of this within 30 days of receipt of the notification. The Data Controller shall only object if the Data Controller has reasonable and specific grounds for such refusal.
What procedures are taken to ensure that sub-processors comply with the data protection standards?	The security measures taken by Amazon Web Servers can be found on their homepage by accessing this link: https://aws.amazon.com/compliance/eu-data-protection/. We monitor and require documentation that sub-processors obtain and maintain external certification.
Privacy by Design	
What are the security measures taken? how does Labster comply with Privacy by Design?	• The LMS connects to the specific learning simulations on the Server API using HTTPS and sends student id, email and name. Nothing else is transmitted from the LMS to Server API, and only HTTPS connections are accepted. • All requests are received by our Load Balancers, which dispatches those request to one of our back-end nodes via SSL. • All external backups are encrypted using PGP. • Django DB Session backend uses a unique cookie which is HTTPONLY = True and Secure = True. • PGP keys are used to encrypt and sign the email with sensitive data. An email policy is in place. • All sensitive data used during deployments is stored using secure vaults and being decrypted only on encrypted partitions on servers protected by a firewall. • LastPass is a tool used by all employees to store and share their passwords securely and only select employees have the necessary level of security to access the storage and SSL management. • The security architecture diagram includes every endpoint that will be part of the project and every connection between endpoints. Every endpoint that listens for connections is identified with its DNS hostname and/or IP address. Every connection is labelled with protocol, encryption type if any, and port number on the listening device. • All sites have QA instances that are sufficiently identical to production that the results of tests in QA can be relied on to evaluate the production instance. • Upgrades to the platform occur frequently, average every 2 weeks. We notify customers of new features and any planned down-time for modifications. • All servers are hosted on Amazon Web Services in similar environments and are completely independent, to ensure no tests affect the production environment. This ensures that any tests performed on sandbox or staging servers will mimic the production environment and ensure minimum risk of deployment-related problems. • Our application server uses Django which has built-in protection against any SQL injection attacks. All queries to databases are further using parameterized arguments to avoid similar attacks. All backups are performed daily as RDS snapshots, and restore capability is tested once every month. • The source code is stored in company private repositories on GitHub, which includes secure automated backup. • All logs are collected to a single service called Papertrail allowing automated audits to identify any malicious or accidental changes. • We are using external libraries in the core foundation of our applications. The main application framework used called Django, it pays attention to security (https://docs.djangoproject.com/en/1.9/topics/security/), follows all current modern trends, and issues prompt bugfix releases on all found security problems (https://docs.djangoproject.com/en/1.8/internals/release-process/). We are using one of the currently supported Django versions in our software. The whole application relies on Django security model, all data interaction is protected by internal Django framework mechanics to protect from typical types of security threats.
Backup processes	
What is your backup process? Are backup media stored off-site? Are backup media strongly encrypted?	• Backups are stored encrypted on Amazon AWS * Backups of backups are stored encrypted in Google cloud. * All files are encrypted with RSA 4096.
Is the backup infrastructure regularly tested to ensure the recoverability of data?	Yes. Once per week, during release testing.

What is the backup strategy?	• All backups are performed daily as RDS snapshots, and restore capability is tested once every month. * Source code is stored in company private repositories on GitHub, which includes secure automated backup. * All logs are collected to a single service called Papertrail allowing automated audits to identify any malicious or accidental changes. * After disposal of service for a given client, all user information for the given client is deleted from the system and from all backups. * All backups are digital
Software Development Life Cycle	
Do systems watch for undesirable or unexpected activity and log these events? Do logged events trigger alerts? What happens then?	We are using Papertrail to collect all logs and OSSEC to watch the potential security threats. OSSEC watches everything and actively monitors all aspects of the Unix system activity with file integrity monitoring, log monitoring, rootcheck and process monitoring. We furthermore use push notifications sent through New Relic and Datadog to inform the entire team of any server issues to ensure fast reaction time
Are current versions of software being deployed? Will upgrades and patches be promptly applied?	We are using Ubuntu operation system with an apt-get command which controls the integrity of installed packages and performs all operations over SSL. Our code repositories are located at GitHub (private access only) and all source code is obtained using ssh protocol. All patches and upgrades are furthermore performed using automated deployment scripts.
Is data secured in transit over the Internet? What are the safeguards?	All data is transferred using TLS. Labster API will refuse to send/receive data for non-validating certificates. All latest security
Is the software under a written Software Development Life Cycle?	We are using external libraries in the core foundation of our applications. The main application framework used called Django, it pays attention to security (https://docs.djangoproject.com/en/1.9/topics/security/), follows all current modern trends, and issues prompt bug fix releases on all found security problems (https://docs.djangoproject.com/en/1.8/internals/release-process/). We are using one of the currently supported Django versions in our software. The whole application relies on Django security model, all data interaction is protected by internal Django framework mechanics to protect from typical types of security threats.
What are your safeguards and procedures to detect/determine whether there has been any compromise of the relevant assets?	• New Relic and DataDog monitoring can show unusual network/CPU activities usually associated with compromises; * We are using Papertrail to collect all logs and OSSEC to watch the potential security threats. OSSEC watches everything and actively monitors all aspects of the Unix system activity with file integrity monitoring, log monitoring, rootcheck and process monitoring. * We furthermore use push notifications sent through New Relic and Datadog to inform the entire team of any server issues to ensure fast reaction time.
Are all events logged with sufficient information to ensure traceability to a unique individual or system?	• All events are logged to local syslog * All syslog events are security transferred to Papertrail cloud service
Is your network infrastructure appropriately designed with segregated zones?	Yes. There is no access from the external network to the internal one.
Will client data be logically segregated from the data of other clients in the cloud?	Yes, on the logical level, while being situated in the same database.
Will our organization be permitted to conduct a vulnerability assessment against the solution environment?	Yes, security scanning (PEN testing) is a typical procedure performed by our customers. To perform such a procedure, the time should be negotiated, and it is usually done against our Staging environment (which is identical to production).
What secure development standards (eg. OWASP, PCI, etc.) are followed in the development of your application?	PCI DSS is validated with a Self-Assessment Questionnaire (SAQ) provided by the PCI Security Standards Council
Vulnerability Program	
Do you have a vulnerability management program for tracking and promptly mitigating security vulnerabilities? What is the timeframe for implementing a critical security fix?	DevOps team monitors security alerts. Also, standard Ubuntu 16.04 system upgrades are encoded into release provision scripts, and so being installed per-release (usually weekly) basis.

Has the new software developed or purchased undergone vulnerability scanning or penetration testing by an entity other than the developer?	Check for security problems is done during code reviews for every new code commit/pull request, and we require a minimum of two coders to do code reviews of each new commit. Software vulnerability and penetration tests are furthermore been performed by internal team members. Finally, we already plan to work with independent parties to do software penetration tests and are researching the market for the best providers of such services.
If our organization identifies a vulnerability in the system, how quickly will you investigate, develop a fix, and apply the fix?	Any security related bugs are treated as hotfixes, and usually installed as soon as hotfix procedure is performed (can be done on the same day).
Data Encryption	
Is data encrypted in storage and/or transmission?	Yes. All sensitive data is encrypted as it travels over each network connection. All connections to Labster services use SSL as transport layer encryption. Our simulations and server setup furthermore enforce the use of HTTPS connections and will prevent any use of insecure HTTP connections by preventing the connection attempt. Furthermore, all internal connections within Labster servers to Amazon RDS databases as well as between nodes within the VPC, are encrypted using SSL, which effectively means 100% of connections are safe. Please refer to the security architecture diagram for a full overview of the secure encrypted connections used throughout the server infrastructure.
How will sensitive data be protected in transit, as it travels across the network?	• All sensitive data is encrypted as it travels over each network connection. * All web sites are using https encryption. Servers have valid https certificates. All connections to Labster services use SSL as transport layer encryption. Our simulations and server setup furthermore enforce the use of HTTPS connections and will prevent any use of insecure HTTP connections by preventing the connection attempt. Furthermore, all internal connections within Labster servers to Amazon RDS databases as well as between nodes within the VPC, are encrypted using SSL, which effectively means 100% of connections are safe.
Is sensitive data (e.g., payment card number, SSN) masked/encrypted such that only authorized individuals have access to the data?	Yes, we use SalesForce and Stripes for payment, and they use widespread industry standards.
Restoration procedures	
How do you restore your web platform from a disaster?	Step-by-step: * Detect affected parts of system and root cause of the issue. * Notify all team members and customers which can be affected about the issue. * Create new instances from pre-created AWS AMI if the cause in hardware, operating system or other software which was not developed by Labster. * Deploy latest stable release to new instances version if AMI's software version is different. * Check and validate configuration files for new instances. * Restore databases from latest successful backups if databases were affected. * Run a smoke test for new instances. * Add new instances to production cluster if new instances were launched. * Run a smoke test for all production cluster. * Prepare an incident report. * Provide steps to prevent such issue in the future. Detailed instructions for each part of the system can be provided by an executive engineer or team which develops affected part of the system.
In case of a database failure, what point in time can you restore the application's data and how long will it take?	We have DB backups every day, restoration DB procedure is up to 1-2 hours.
Data Security	
How is the security architecture diagram?	The security architecture diagram includes every endpoint that will be part of the project and every connection between endpoints. Every endpoint that listens for connections is identified with its DNS hostname and/or IP address. Every connection is labelled with protocol, encryption type if any, and port number on the listening device.

How will sensitive data be protected at rest, wherever it is stored?	• All production servers and backups are located within Amazon Web Services. * All databases and database backups are stored using encrypted RDS instances. * All developers that have access to production and backup databases never use databases with sensitive information for local development. * All local hard drives used by developers are although still also encrypted.
Data Destruction	
What measures are taken to ensure that data is securely destroyed?	The data is not automatically removed. Data destruction is implemented by a one-time command which is run by the system administrator. After disposal of service for a given client, all user information for the given client is cleaned up from the system and from backups. After deletion of information for the given client from backups, backups are archived and encrypted. Backups are digital. This is part of our Secure Software Development Life Cycle.
Do you have plans for data retention and proper disposal?	After disposal of service for a given client, all user information for the given client is cleaned up from the system and from backups. After deletion of information for the given client from backups, backups are archived and encrypted. Backups are digital. This is part of our Secure Software Development Life Cycle.
Data Storage	
Where are the personal data stored?	The geographical location of Amazon Web Servers in the United Kingdom and in United States (protected through EU-US Privacy Shield).
Data transfer	
Is data transferred to third parties?	Personal data is never shared with third parties or agents. We handle all data management, backups and servers internally, hosted on Amazon Web Services. Amazon is our sub-processor and there is a data agreement signed between Labster and Amazon.
Data Breach	

What procedures are taken to ensure that data breaches are detected?	Labster has already taken and continues to take the highest security measures with employees and systems. Internally, Labster has a clear process of reporting, escalating and fixing issues. Essentially, a few severity inputs (e.g. level of security breach, number of users affected) are evaluated and mapped to one of four priority response levels by our Escalation Team (internal bug masters and security roles) that determine if and how we fix our systems immediately or align a fix with our continuous release plan. **Problem Severity Level 1** - This Problem Severity Level is associated with: (a) one or more Activities are non-functional or not accessible to more than 30 users; (b) unauthorized exposure of all of part of user data; or, (c) loss or corruption of all or part of user data. * Request Response Time. 1 working day. * Request Resolution Time. 2 working days. **Problem Severity Level 2** - This Problem Severity Level is associated with significant and/or ongoing interruption of a user's use of one or more Activities and for which no acceptable workaround is available. * Request Response Time. 1 working day. * Request Resolution Time. 9 working days. **Problem Severity Level 3** - This Problem Severity Level is associated with minor and/or limited interruption of a user's use of one or more Activities. * Request Response Time. 1 working day. * Request Resolution Time. 14 working days. **Problem Severity Level 4** - This Problem Severity Level is associated with general questions pertaining to the Activities, or other issues which are not included in Problem Severity Levels 1, 2, or 3, and which Pearson cannot address via their direct support, as stated in 5.1. * Request Response Time. 1 working day. * Request Resolution Time. 2 working days.
What procedures are taken to ensure that data breaches are reported?	As soon as a data breach is identified, our partners and customers will be notified about the breach and the estimated impact. Following this, we assess the impact and write a full report on the data that has been breached, which is shared only with our partners and customers. Together with our partners and customers, we then determine the best process to inform end -users of the data breach and provide recommendations (such as changing user passwords).
Documentation	
Is a central record of processing activities maintained in a format that can be used to demonstrate processing activities to the controller? If you have a central record, how often is this reviewed and updated?	Yes, we do - we store our records of processing activities in Atlassian. It is updated as part of our change process.
Customer communication	
Changes to the privacy policy	Changes to privacy policies are communicated by the Customer Success team. If there are any changes to our privacy policy, we will announce that these changes have been made on our home page and on other key pages on our site. If there are any changes in how we use our site customers' Personally Identifiable Information, notification by e-mail or postal mail will be made to those affected by this change. Any changes to our privacy policy will be posted on our web site 30 days prior to these changes taking place.
How will individuals be told about the use of their personal data?	Labster terms and conditions web page will be linked in each Moodle course where Labster simulations are available. https://www.labster.com/terms-and-conditions/ This goes for both institutions as well as individual licenses purchased by customers, all are presented with a dialogue box in which they need to accept terms and conditions.
How often is the application modified and how do you notify your customers of an upcoming modification?	Upgrades to the platform occur frequently, average every 2 weeks. We notify customers of new features and any planned downtime for modifications.

Cookies Policies	Our Site may use “cookies” to enhance User experience. User’s web browser places cookies on their hard drive for record-keeping purposes and sometimes to track information about them. The user may choose to set their web browser to refuse cookies or to alert you when cookies are being sent. If they do so, note that some parts of the Site may not function properly.
Right to erasure communication	If you would like to erase your personal identification information from Labster database, please contact support@labster.com. By performing this request, all data will be removed and this includes, but not limited to, when users visit our site, register on the site, log into the virtual laboratory, complete laboratory steps, subscribe to the newsletter, respond to a survey, fill out a form, and in connection with other activities, services, features or resources we make available on our Site. All the personal identification information such as name, email address, mailing address, and/or phone number will also be erased.
Right to be forgotten	
Removing customer data	If a customer wishes their data to be removed, it will be processed through a manual command. This process is the same for all types of customers, institutions as well as individual customers. A customer is removed from the running system.
Removing customer data from backups	We do not remove (and cannot) from backups. Labster backups have certain expiration time - 2 months. Labster does not store data older than 2 months in the backup folders. (this is aligned with our automatic LifeCycle rules and has been confirmed in Google Cloud and Amazon Cloud).