EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. **Purpose**

(a) This Exhibit supplements the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES' website.

(b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

(d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy.. Erie 1 BOCES will provide Vendor with a copy of its policy. Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA: See attached STEM Sims Data Security and Privacy Policies.

(c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(e) Vendor [*check one*] ______will ___X___will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:

(i) the parent or eligible student has provided prior written consent; or

(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

(a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).

(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department

("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

(e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available for public review at **http://www.nysed.gov/data-privacy-security/student-data-inventory**, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website **http://www.nysed.gov/data-privacy-security/report-improper-disclosure**.

BY THE VENDOR:

Monica Murphy
Signature

Monica Murphy
Printed Name

President and CEO
Title

10/13/2022
Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND STEM SIMS, LLC

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with STEM Sims, LLC which governs the availability to Participating Educational Agencies of the following Product(s):

STEM Sims

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: N/A, no subcontractors will be utilized

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on February 1, 2022 and expires on June 30, 2025.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

wnyric
www.wnyric.org
Erie 1 BOCES Education Campus • 355 Harlem Road • West Seneca, NY 14224-1892

erie boces

STEM Sims

STEM Sims Data Security and Privacy Policies

Approving Officer: Monica Murphy, Chief Executive Officer
Approval Date: August 18, 2021
Advisor: Raymond Bernardo, Chief Technology Officer
Next Scheduled Review: August, 2022
Description: This plan establishes the steps to secure and protect online Personal Confidential Information.

Monica AB Murphy

August 18, 2021
Approval Signature and Date

1. Data Classification and Privacy

a. Definitions

Data Security - Data security describes how to protect personal data from any unauthorized third-party access or malicious attacks and exploitation of data. It is set up to protect personal data using different methods and techniques to ensure data privacy.

Data Privacy - Data privacy describes the proper handling, processing, storage, and usage of personal information.

Confidential Information – means: (a) Protected Information, (b) any personally identifiable information related to users (students, employees, agents and/or volunteers), (c) all findings, analysis, data, reports, or other information, whether in oral, written, graphic, or machine-readable form, obtained from user or furnished by the users in connection with the Services, and (d) all information marked "confidential" in writing.

Process or Processing - means to perform any act, omission, or operation on or with respect to data or information, such as accessing, adapting, altering, blocking, collecting, combining, delivering, deleting, destroying, disclosing, disseminating, erasing, generating, learning of, organizing, recording, releasing, retrieving, reviewing, sharing, storing, transmitting, using, or otherwise making data or information available.

Protected Information – means (a) information about users' current, future, and former students and their families, consists of "personally identifiable information" as defined by the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g and its implementing regulations, 34 C.F.R. Part 99 ("FERPA") and (b) as it relates to users, consists of "personally identifying information."

Personally Identifiable Information (PII) - PII is information about an individual maintained by an agency, including: 1) Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records, 2) Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Authorized Users - STEM Sims shall only disclose Confidential Information to its defined users and its nonemployee agents, assignees, consultants, or subcontractors who need to Process the Confidential Information in order to carry out the Services and in those instances only to the extent justifiable by that need.

b. Data Security and Privacy Plan Overview

STEM Sims will neither retain nor incorporate any of the Confidential Information into any database or any medium other than that which may be required for it to provide the Services and agrees to maintain appropriate administrative, technical, and physical safeguards in accordance with industry best practices and applicable law to protect the security, confidentiality, and integrity of Protected Information in its custody.

STEM Sims technologies, safeguards and practices align with the NIST Cybersecurity Framework, and include sufficient (A) data privacy protections, including processes to ensure that Personally Identifiable Information is not included in public reports or other public documents; and (B) data security protections, including data systems monitoring, encryption of data in motion and at rest, an incident response plan, limitations on access to Protected Information, safeguards to ensure Protected Information is not accessed by unauthorized persons when transmitted over communication networks, and destruction of Protected Information when no longer needed. STEM Sims uses encryption technology to protect Protected Information while in motion or in its custody from unauthorized disclosure and conducts digital and physical periodic risk assessments and to remediate any identified security and privacy vulnerabilities in a timely manner.

c. Confidential Information

STEM Sims holds Confidential Information in strict confidence and does not disclose it to any third parties nor make use of such Data for its own benefit or for the benefit of another, or for any use other than the purpose agreed upon. STEM Sims uses commercially reasonable efforts to secure and defend any System housing Confidential Information against third parties who may seek to breach the security thereof, including, but not limited to, breaches by unauthorized access or making unauthorized modifications to such System.

STEM Sims protects and secures all Confidential Information in transit (collected, copied, and moved) and at rest (stored on the physical servers), including during any electronic data transmission or electronic or physical media transfer. STEM Sims maintains all copies or reproductions of Confidential Information with the same security it maintains the originals. At the point in which the Confidential Information is no longer useful for its primary or retention purposes, the information will be destroyed, making it unusable and unrecoverable.

STEM Sims maintains accurate legal name, address, phone number information for all users who are permitted to access Confidential Information and, upon request, can produce lists of users who will have access to Confidential Information. All Application screens of reports and landing pages of web Applications that contain Confidential Information include prominent confidentiality notices in legible-sized font on each page and are non-cacheable. Confidential Information does not appear in Application URLs. All STEM Sims development, test and QA environments do not use real Confidential Information.

d. Electronic Payment Protection

STEM Sims adheres to the following guidelines when accepting and processing electronic payments from users: 1) Cardholder data is not stored on the systems or in written form, 2) All cardholder data are entered into a secured third-party payment system, such as Square or PayPal, 3) Never request cardholder information to be transmitted via email or any other electronic communication system, 4) Payment information shall be entered directly into the approved payment system by individual making payment. If the individual is not able to directly input the payment, designated staff may gain verbal approval for the payment process either in person or via phone (after identification is verified). If verbal payment information is received, that information must be entered directly into the payment system and not written down during the process. If payment information is collected via a physical form, that form must be shredded or other payment information destroyed immediately after its intended use.

2. Security Training and Awareness

a. Awareness

The Chief Technology Officer is responsible for the awareness of and the maintaining and implementing of training programs to support staff in their understanding of data security and data privacy.

b. Training

STEM Sims maintains a data security training program for new and existing employees. The program consists of the following: 1) Training for all staff on technology policies and procedures, including confidentiality and data privacy, 2) Training for staff on federal regulations and the use of digital resources and student electronic records, 3) Training on the protection from the latest malware, phishing, and other resources that might compromise systems.

3. Systems Administration

STEM Sims provides access to Confidential Information to users only when access is necessary for the performance of their duties and discloses Confidential Information only to authorized users or agents who need access to the information to provide services and who agree not to disclose the information to any other party except as allowed by law. Therefore, systems access will only be given on an as-needed basis as determined by the Chief Technology Officer.

4. Application Development and Code Review

a. Development

STEM Sims uses a comprehensive secure development lifecycle system consistent with industry standard best practices, including policies, training, audits, testing, emergency updates, proactive management, and regular updates to the secure development lifecycle system itself. STEM Sims's handling of Confidential Information complies with secure coding standards. STEM Sims reviews and tests all application code for security weaknesses and backdoors prior to deployment. All high-risk findings and exploitable vulnerabilities are resolved before the Application is released. STEM Sims has explicitly defined authorization controls that prevent users from exceeding their intended privileges and perform authorization checks before performing any action that creates, views, updates, transmits or deletes Confidential Information. Authorization checks verify the user has appropriate role to perform the requested action, and the correct scope.

b. Code Review and Resolution

STEM Sims makes use of a Code-Review-Revise-Review-Test process in which every change is extensively reviewed and tested by at least one other software engineer.

STEM Sims responds to and resolves security-related bug reports, inquiries, and incidents in a timely and professional manner. Notifications of such incidents are made within 24 hours of becoming aware of any such incident that poses a potential risk to data.

c. Systems Security

STEM Sims enforces a one user, one account policy in which shared/group accounts and duplicate accounts are not permitted. STEM Sims does not allow testing, development, and non-production accounts. STEM Sims enforces a strong password policy of five characters minimum entered into a non-display field and stores all passwords in a non-reversible one-way cryptographic hash and offers a secure password reset feature and tool, including verification of identity, email or text notification, and a one-time-use password link that expires after 24 hours. STEM Sims logs all successful and failed authentication attempts, including date, time, IP address, and username and temporarily locks accounts with repeated failed login attempts and provides support to affected users. Users are encouraged to change their passwords every 90 days. Users and staff who have reason to believe a password is lost or compromised must notify the Chief Technology Officer or designee as soon as possible.

All STEM Sims Systems that Handle Confidential Information encrypt the Confidential Information data in transit using algorithms and key lengths consistent with the most recent NIST guidelines. For HTTP and other protocols that use SSL/TLS, the TLS 1.2 or later protocols with 128- bit or larger key size will be used and make previous protocols and smaller keys unavailable.

d. Third-Party Providers

STEM Sims utilizes the third-party provider Let's Encrypt, which is a recognized and trusted authority in the industry, to generate SSL certificates that are used for authentication between the server and the user. All private keys are kept confidential, and implementations are in place for key lifecycle management and the protection of all keys in storage or in transit.

If a user application requires Single Sign-On (SSO) integration, STEM Sims works with user groups to support authentication for users.

5. Incident Response Plan

Please see the *STEM Sims Data Breach Response Plan* Document.

6. Workstation Management

a. Workstation Protection

All workstations run macOS which gives us access to their full suite of security services. All workstations are fully encrypted utilizing FileVault. Once a workstation's data is encrypted it cannot be accessed without the employee's password.

b. Acquisition of New Equipment

The acquisition of new equipment follows a stepwise process that: 1) ensures the security of existing systems, 2) increases data integration capabilities and efficiency, and 3) minimizes the inadvertent downloading of malicious code.

c. Systems Protection

All STEM Sims operating Systems, servers, and network devices that support Confidential Information are kept hardened and patched. All security-related patches are installed on Systems within a reasonable timeframe.
The Internet traffic from all devices on the internal network is routed through a firewall and content filter. Filtering levels are based on the role of the user. All sites that are known for

malicious software, phishing, spyware, etc. are blocked. Email is filtered for viruses, phishing, spam, and spoofing using Fastmail services. A multi-layered approach is used to ensure that all electronic files are appropriately scanned for viruses, malware, spyware, phishing and SPAM. These include, but are not limited to, enterprise virus/malware/ spyware software, group policy, gateways, firewalls, and content filter. Users shall not turn off or disable protection systems or install other systems.

d. Security Training

STEM Sims maintains a data security training program for new and existing employees. The program consists of the following: 1) Training for all staff on technology policies and procedures, including confidentiality and data privacy, 2) Training for staff on federal regulations and the use of digital resources and student electronic records, 3) Training on the protection from the latest malware, phishing, and other resources that might compromise systems.

7. Backups, Disaster Recovery, and Business Continuity

a. System Backups

i. Internal Network

Internal network systems are installed in an access-controlled area. The area in and around the computer facility affords protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations. The area is monitored and maintains the data centers' temperature and humidity levels.

Computers and other systems shall be secured against use by unauthorized individuals. It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use.

ii. External Network

File servers and/or storage containing PII, Confidential and/or Internal Information are installed in a secure off-site location and area to prevent theft, destruction, or access by unauthorized individuals. This ensures network systems and network equipment are properly secured to prevent unauthorized physical access and data is properly safeguarded to protect from loss.

b. Disaster Recovery

STEM Sims's Technology Disaster Recovery Plan includes processes that enable continued operations and efficiently restore any loss of data in the event of fire, vandalism, natural disaster, or critical system failure. The objectives during a natural disaster or critical failure are the following:

- Minimize the loss or downtime of core systems and access to data.
- Recover and restore critical systems and data.

- Maintain essential technology resources critical to day-to-day operations.
- Minimize the impact to users during or after a critical failure.

STEM Sims data is all stored externally and uses cloud-based backups. Snapshot copies of the critical virtual servers are performed regularly. In the event of a critical system failure, STEM Sims will restore that server back to our current environment from the backup solution.

c. Business Continuity

The STEM Sims Application along with the Systems that Handle Confidential Information are available and fully functional 24x7x365 with 99.9% uptime unless unforeseen issues, such as natural disasters, arise. STEM Sims will notify users of any major planned interruptions in service, with the exception of emergency security updates.

8. Requirements for Third-Party Partners

In the event that STEM Sims utilizes subcontractors to support a System that Handles Confidential Information (such as the WEB Host: DigitalOcean), such subcontractors are subject to, and are required to comply with, the requirements set forth herein.

9. Compliance

STEM Sims agrees to hold all Confidential Information it Processes in compliance with all applicable provisions of federal, state, and local law, including but not limited to FERPA and any applicable regulations promulgated thereunder. STEM Sims understands that the disclosure of Protected Information to persons or agencies not authorized to receive it is a violation of United States federal law and some state law, which may result in civil and/or criminal penalties.

STEM Sims, upon reasonable notice, allows state and/or federal authorities to perform security assessments or audits of Systems that Handle or support Confidential Information. Such an assessment shall be conducted by an independent 3rd party agreed upon by STEM Sims and the authorities, and at the authorities' own expense. STEM Sims will cooperate with any such assessment/audit and shall, at its own expense, provide all necessary support, personnel, and information needed to ensure the successful completion of the assessments or audits. STEM Sims agrees to provide, upon reasonable requests, reports relating to the protection of Confidential Information and safeguards implemented in its organization.

In the event of adverse findings through an audit, STEM Sims shall cooperate with the authorities in remediating any risks to Confidential Information, including complying with request to temporarily taking the System offline or otherwise limiting access to the System, and any other follow up actions reasonably necessary to secure the Confidential Information.

10. Revisions/Changes to Policies

Changes, other than those specified by new local, state, or federal regulations and/or laws will not be made to the herein policies without informing all user groups of intended changes to policies.