

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 and 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: Apptegy maintains comprehensive security practices and policies, including industry-accepted administrative, operational, technical, and physical security controls and safeguards. These align with the NIST Cybersecurity Framework. Our practices and policies promote the security of the services and the availability, integrity, and confidentiality of Personally Identifiable Information in our care. We review our practices and policies at least annually and update them as appropriate. Examples of relevant safeguards and practices that Apptegy uses and maintains include: encryption of information in transit and at rest; Role-Based Access Control (RBAC) principles (to determine and help ensure appropriate access, use, and processing of Personally Identifiable Information and limit internal access to Personally Identifiable Information to only those employees or Third Parties that need access to provide our services); vulnerability monitoring and remediation; formal security

incident response plans; written confidentiality obligations with employees and Vendors to whom Aptegy may disclose Personally Identifiable Information; and employee security and privacy training for new employees and periodic security and privacy training for existing employees

- (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*] X will 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)**ERIE 1 BOCES****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>.

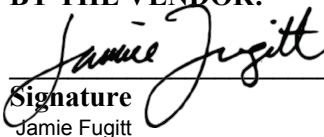
BY THE VENDOR:**Signature**
Jamie Fugitt**Printed Name**
Chief Legal Officer, Apptegy, Inc.**Title**
11/07/2023**Date**

EXHIBIT D (CONTINUED)**Supplemental Information**

about the Master License and Service Agreement
 between
 Erie 1 BOCES and Apptegy

Erie 1 BOCES has entered into a Master License and Service Agreement (“MLSA”) with Apptegy which governs the availability to Participating Educational Agencies of the following Product(s):

Thrillshare software-as-a-service platform

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: When Vendor engage a subcontractor to perform its contractual obligations under the MLSA, the data protection obligations imposed on Vendor by state and federal law, and contract (including without limitation the MLSA and this Exhibit D), will apply to the subcontractor. For avoidance of doubt, 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 extending the equivalent data security and privacy standards required of Vendor under the MLSA and applicable state and federal law, including without limitation those obligations contained within Section 2-d of the New York State Education Law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by measures including, without limitation: performing risk assessments on new and existing subcontracts at least annually and updating such subcontractor’s agreements with vendor as appropriate and required to ensure such subcontracts with access to Protected Data are bound by written confidentiality obligations.

Duration of MLSA and Protected Data Upon Expiration:

The MLSA commences on the date it is executed by both parties and expires on June 30, 2026.

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 commercially reasonable 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, feasible, and commercially reasonable 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.

EXHIBIT D (CONTINUED)

APPTegy DATA SECURITY AND PRIVACY PLAN**I. Introduction**

This Data Security and Privacy Plan (the “**Plan**”) supplements and is in addition to the Master Services Agreement (the “**Services Agreement**”) of Apptegy, Inc. (together with its affiliates, agents, and assigns, “**Apptegy**” or “**we**”). As required by Part 121.6(a) of Section 2-d of the New York State Education Law, the Plan should be considered included in any Services Agreements or other relevant agreements between Apptegy and any Educational Agencies (“**Educational Agencies**” or “**you**”), within the meaning of and as defined in Part 121 of Section 2-d of the New York State Education Law (the “**NYS Education Law**”). This Plan applies to Apptegy and its relationship with the Educational Agencies. A capitalized term that is used but not specifically defined in this Plan will have the meaning given to that term in Section 121.1 of the NYS Education Law.

II. Components of Plan as Required by the NYS Education Law

1. **Explanation of How Apptegy Will Implement All State, Federal, and Local Data Security and Privacy Contract Requirements Over the Life of Services Agreements (NYS Education Law §121.6(a)(1)):**

Apptegy will perform its obligations under Services Agreements in compliance with all state, federal, and local data security and privacy contract requirements (including the NYS Education Law).

2. **Explanation of the Administrative, Operational, and Technical Safeguards and Practices Apptegy Has in Place to Protect Personally Identifiable Information (NYS Education Law §121.6(a)(2)):**

Apptegy maintains comprehensive security practices and policies, including industry-accepted administrative, operational, technical, and physical security controls and safeguards. These align with the NIST Cybersecurity Framework. Our practices and policies promote the security of the services and the availability, integrity, and confidentiality of Personally Identifiable Information in our care. We review our practices and policies at least annually and update them as appropriate. Examples of relevant safeguards and practices that Apptegy uses and maintains include: encryption of information in transit and at rest; Role-Based Access Control (RBAC) principles (to determine and help ensure appropriate access, use, and processing of Personally Identifiable Information and limit internal access to Personally Identifiable Information to only those employees or Third Parties that need access to provide our services); vulnerability monitoring and remediation; formal security incident response plans; written confidentiality obligations with employees and Vendors to whom Apptegy may disclose Personally Identifiable Information; and employee security and privacy training for new employees and periodic security and privacy training for existing employees.

3. **Explanation of How Apptegy will Comply With the Requirements of §121.3(c)(1-6) (NYS Education Law §121.6(a)(3))**

i. **Explanation of the Exclusive Purposes for Which Student Data or Teacher or Principal Data Will Be Used (NYS Education Law §121.3(c)(1)):**

Apptegy will use Student Data and Teacher or Principal Data exclusively and only to the extent explicitly authorized in Services Agreements – specifically, providing Apptegy’s products and services to Educational Agencies and facilitating Educational Agencies’ use of Apptegy’s products and services.

Apptegy does not sell Personally Identifiable Information nor use or disclose it for any Commercial or Marketing Purpose or facilitate its use or disclosure by any other party for any Commercial or Marketing Purpose or permit another party to do so.

ii. **Explanation of How Apptegy Will Ensure That Any Subcontractors to Whom Apptegy May Disclose Student Data or Teacher or Principal Data Will Abide by All Applicable Data Protection and Security Requirements (NYS Education Law §121.3(c)(2)):**

Apptegy may use subcontractors (“**Third Parties**” or “**Vendors**”) in connection with Services Agreements. Apptegy will only disclose Student Data and Teacher or Principal Data in accordance with and as permitted by applicable state or federal law (including the NYS Education Law). We limit the Student Data and Teacher or Principal Data we disclose to Third Parties as much as possible. When we disclose Student Data or Teacher or Principal Data with a Third Party, the Third Party is allowed to access or use the Student Data and Teacher or Principal Data that is needed to do their particular work with us and is not allowed to access or use additional Student Data or Teacher or Principal Data. When Apptegy engages a Third Party, the data protection obligations imposed on Apptegy by state and federal law and contract will extend to such Third Parties that receive or have access to Student Data or Teacher or Principal Data.

Apptegy uses Third Parties to enable certain technical features of our products and services, and to secure and protect our products and services, via Third-Party software tools that we implement in our systems. For new Vendors that will receive or have access to Student Data or Teacher or Principal Data, we perform a risk assessment before we begin using the Vendor’s product or service. Apptegy also performs risk assessments on existing Vendors at least annually. We update our Vendors and/or Vendor agreements, as appropriate, based on our Vendor risk assessments. Vendors with access to Student Data or Teacher or Principal Data are bound by written confidentiality obligations and access and use limitations.

iii. **Description of the Duration of Services Agreements and What Will Happen to the Student Data or Teacher or Principal Data Upon Expiration of Services Agreements (NYS Education Law §121.3(c)(3)):**

The duration of our Services Agreements is as set out expressly therein. Services Agreements may be renewed for additional terms in accordance with their terms and conditions. Upon termination or expiration of a Services Agreement, Apptegy will work with an Educational Agency to promptly (i) return Student Data and Teacher or Principal Data to the applicable Educational Agency; (ii) delete and/or destroy Student Data and Teacher or Principal Data; or (iii) transition Student Data and Teacher or Principal Data to a successor contractor of the Educational Agency.

iv. **Explanation of How a Parent, Student, Eligible Student, Teacher or Principal May Challenge the Accuracy of Student Data or Teacher or Principal Data Collected by Apptegy (NYS Education Law §121.3(c)(4)):**

Any individual who has verifiable authority to act on behalf of an Educational Agency may contact Apptegy as set out below in Section III for any question related to the accuracy of Student Data or Teacher or Principal Data. Apptegy will verify the identity and authority of all individuals making any such request before processing and addressing the request. Apptegy reserves the right to require that any such request be made in writing and reserves the right to decline or limit these requests in certain circumstances – for example, when we are unable to verify an individual’s identity or authority to make such a request on behalf of an Educational Agency.

Any individual acting on behalf of himself or herself (including a parent or a student) or acting on behalf of any other party other than a verified request on behalf of an Educational Agency, must direct all requests for access or any other question related to Student Data or Teacher or Principal Data to an Educational Agency directly, in accordance with NYS Education Law §121.12(c).

v. **Explanation of Where Student Data or Teacher or Principal Data Will Be Stored (NYS Education Law §121.3(c)(5)):**

Apptegy uses Amazon Web Services (“AWS”) to host and facilitate our products and services. We store client data for United States clients in AWS servers located in the United States. AWS provides these services to millions of active customers, specifically including educational institutions (including Harvard University, Notre Dame, the University of Texas, and the University of California System, among others). AWS supports more security standards and compliance certifications than any other hosting provider, including ISO, SOC2, NIST, GDPR, PCI-DSS, and others.

vi. **Explanation of How Data Will Be Protected Using Encryption While in Motion and at Rest (NYS Education Law §121.3(c)(6)):**

Apptegy protects data with industry-accepted encryption in transit and at rest (for example: 256-bit AES encryption and NIST SP 800-57).

4. **Explanation of How Officers, Employees, and Assignees of Apptegy Who Have Access to Student Data or Teacher or Principal Data Receive Training on Laws Governing Confidentiality of Such Data Prior to Receiving Access (NYS Education Law §121.6(a)(4)):**

Each Apptegy officer, employee, and assignee who has access to Student Data or Teacher or Principal Data receives training on laws governing confidentiality of such data (i) as part of such individual’s initial orientation training, and (ii) annually in accordance with our ordinary practices, and (iii) periodically on an as-needed basis (for example: when changes to applicable law mandate an update to or revision of our practices). Training may be delivered in person and/or using online training tools. Additionally, Apptegy employees are bound by written confidentiality obligations with respect to Student Data and Teacher or Principal Data.

5. **Explanation of How Apptegy Will Manage Its Relationships and Contracts With Third Parties to Ensure Personally Identifiable Information Is Protected (NYS Education Law §121.6(a)(5)):**

Apptegy may use Third Parties in connection with Services Agreements. We limit the Personally Identifiable Information we disclose to Third Parties as much as possible. When we disclose Personally Identifiable Information with a Third Party, the Third Party is allowed to access or use the Personally Identifiable Information that is needed to do their particular work with us and is not allowed to access or use additional Personally Identifiable Information. When Apptegy engages a Third Party, the data protection obligations imposed on Apptegy by state and federal law and contract will extend to such Third Parties that receive or have access to Personally Identifiable Information.

For new Vendors that will receive or have access to Personally Identifiable Information, we perform a risk assessment before we begin using the Vendor’s product or service. Apptegy also performs risk assessments on existing Vendors at least annually. We update our Vendors and/or Vendor agreements, as appropriate, based on our Vendor risk assessments. Vendors with access to Personally Identifiable Information are bound by written confidentiality obligations and access and use limitations.

6. Explanation of How Apptegy Will Manage Data Security and Privacy Incidents That Implicate Personally Identifiable Information (NYS Education Law §121.6(a)(6)):

Apptegy maintains formal security incident response plans. Our practices are designed to detect, stop, investigate, and remediate known and suspected security incidents promptly. In the event of any breach or unauthorized release of Personally Identifiable Information, we will notify impacted Educational Agencies of verified security incidents in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after the discovery of such breach, and Apptegy will work with impacted Educational Agencies to complete all incident response actions as required of them by law, if any. Apptegy also cooperates with Educational Agencies and law enforcement to protect the integrity of any investigations into a breach or unauthorized release of Personally Identifiable Information. Where a breach or unauthorized release is attributed to Apptegy, Apptegy will pay or promptly reimburse the Educational Agency for the full cost of the Educational Agency's notification requirements under NYS Education Law §121.10. Apptegy also conducts internal, post-incident reviews for security incidents and works to reduce the likelihood of similar incidents in the future.

7. Explanation of How and When Data Will Be Returned, Transitioned, or Deleted or Destroyed by Apptegy When a Services Agreement Is Terminated or Expires (NYS Education Law §121.6(a)(7)):

Upon termination or expiration of a Services Agreement, Apptegy will work with an Educational Agency to promptly (i) return data to the applicable Educational Agency; (ii) delete and/or destroy the Educational Agency's data; or (iii) transition the data to a successor contractor of the Educational Agency.

III. Contact Us

If you have questions about this Plan or any related matter, please contact us at any of the following:

- By email at privacy@apptegy.com; or
- By telephone at 1-888-501-0024; or
- By mail at Apptegy, Inc., c/o Data Protection Officer, 2201 Brookwood Dr., STE 115, Little Rock, AR 72202.

EXHIBIT E

Apptegy Service Level Agreement

This service level agreement (the “**SLA**”) supplements and is in addition to your agreement (the “**Services Agreement**”) with Apptegy, Inc. (together with its affiliates, agents, and assigns, “**Apptegy**” or “**we**”) (collectively the “**Parties**”). More specifically, this SLA explains the measures Apptegy will take to help ensure the appropriate functionality and availability of the “**Services**” pursuant to the Services Agreement, and your rights in the event of potential interruptions in or unavailability of the Services. The effective date of this SLA will be the effective date of the Services Agreement, and it will terminate on the termination or expiration of the Services Agreement.

Your use of the Services will continue to be subject to the terms and conditions of the Services Agreement, which includes and incorporates Apptegy’s Terms of Use (the “**TOU**”) and Privacy Policy (the “**Privacy Policy**”), which can be found at www.apptegy.com/terms-and-conditions/ and www.apptegy.com/privacy-policy/, respectively.

1. Definitions. The terms below are defined as follows:

Component: A Component is each individual feature or function of the Services that is integral to your educational or business mission (e.g., your website, mobile app, Thrillshare, Media, Rooms).

Uptime: Uptime is the amount of time that each Component of the Services is available to you and operating as intended without substantial interruption, plus any scheduled or emergency maintenance. Uptime is calculated for each individual component on a percentage basis and is measured over each calendar month to the nearest minute based on the number of minutes in the month (for instance, a 31-day month contains 44,640 minutes). The guaranteed Uptime for each component of the Services is 99.9% (roughly 44,595 minutes in a 31-day month). Uptime percentage is calculated according to the following formula:

$$[(\text{total minutes in month} - \text{Downtime}) / \text{total minutes in month}] > 99.9\%$$

Downtime: Downtime is the amount of time for each Component that you are either unable to access or use it without substantial interruption (in other words, “application failure”). Downtime, however, does not include time when the Services are unavailable or not functioning properly through your own fault or other excluded causes listed below in section 3. Like Uptime, Downtime is calculated as a percentage based on the number of minutes in any given month.

Credit: A Credit is how we will compensate you for any Downtime you may experience exceeding the 99.9% Uptime threshold for a Component.

Scheduled Maintenance: Scheduled Maintenance is any regularly scheduled maintenance that we perform to help ensure the integrity and functionality of the Services. We will use commercially reasonable efforts to ensure we give you reasonable notice before conducting such maintenance, and that it is conducted during non-business hours or hours of low usage (usually after 8:00 p.m. CST).

Emergency Maintenance: Emergency Maintenance includes maintenance we conduct but could not have reasonably anticipated based on the circumstances. Like our approach to Scheduled Maintenance, we will use commercially reasonable efforts to give you as much advance notice of Emergency Maintenance as is reasonable and practical.

2. Support Requests. When you request support from Apptegy, it should be through our online support services, support email (support@apptegy.com), or support phone number (501-613-0370). Upon receipt of your request, we will respond as soon as possible, and use commercially reasonable, appropriate measures to minimize or resolve any errors or interruptions.

Given the nature of our products and services, we cannot provide guaranteed, precise response or resolution times. Subject to that limitation, our standard support team hours are 8:00 a.m. – 5:00 p.m. CST, Mondays through Fridays. We almost always respond to requests made on weekdays between 12:00 a.m. – 4:30 p.m. CST on the same calendar day, and generally respond to *any* request no later than the beginning of the next support team shift. For purposes of example only, our average response time to requests made during standard support hours is just under two (2) minutes, and most requests for support are closed within thirty (30) minutes (irrespective of an issue’s type or cause).

Response times are measured from the moment the request is received and the moment we reply to the request, whether that is to provide a solution or to get more information.

3. Services Covered. This SLA covers only those services provided by Apptegy to you pursuant to your Services Agreement. Additionally, any unavailability or loss of functionality resulting from the following will not be included in the calculation of Downtime:

- Interruptions resulting from user error (your own fault), including if you use the Services in a manner not contemplated by, or that otherwise violates, the Services Agreement;
- Interruptions caused by “force majeure” events, or other events reasonably outside our control. This would include, but is not limited to, natural disasters (e.g., floods or pandemics); war or other governmental interruptions; interruptions in utility services such as electricity and telecommunications including internet connectivity issues; and interruptions to physical tools or equipment that we do not own or control;
- Interruptions caused by or related to third parties, including third-party services, networks, or tools, such as those integrated with our Services to provide certain functions (although we will use reasonable efforts to help communicate and resolve issues with relevant third parties, such interruptions will almost always be beyond our control and thus no guarantees can be made); and
- Interruptions resulting from Scheduled Maintenance and Emergency Maintenance, which are excluded when calculating the Downtime for a Component.

4. Uptime Guarantee and Service Credits. As indicated, we guarantee a service level of 99.9% Uptime for each Component, as calculated on a monthly basis. In the event the Uptime for a given Component fails to meet the 99.9% service level threshold for any calendar month, you will be entitled to a Credit for the Downtime.

Service Levels Service Credits

<99.9% but greater than or equal to 99.0%	= 1%
<99.0% but greater than or equal to 95.0%	= 5%
<95.0% but greater than or equal to 90%	= 15%
<90.0%	= 25%

For each calendar month during which we fail to meet the 99.9% service level, you will be entitled to receive a Credit equal to the percentage of fees that you actually paid to us for the affected Services for that month, as identified in the service level table above. Credits, if applicable, will be applied to your renewal invoice at the end of your then-current subscription term, or added on to the end of your then-current subscription term if you decide not to renew your Services with Apptegy.

You must request any Credit within ten (10) days following the end of the calendar month in which a failure occurred. When you notify us, you must also provide us with a sufficient description of the affected Component(s), the date(s), time(s), and duration(s) of the Downtime in writing. Note, however, that if we disagree with your calculation, we will provide you with an alternate calculation using our own service monitoring tools and equipment, and our determination of the Downtime percentage and potential Credit will be final. Notwithstanding the foregoing, we will first attempt to discuss with you and reach a mutually agreeable calculation before making a final determination as to the amount of Credit.

Credits are not refunds. As such, they cannot be exchanged into a cash amount. In addition, Credits are capped at a maximum of thirty (30) days of paid service, require you to have paid any outstanding invoices, and expire upon the termination of your Services Agreement. Excluding the remedies associated with any breach of warranty under the Services Agreement, the remedies set out in this section will be Apptegy's sole obligation and your exclusive remedy with respect to any failure by us to meet the applicable service levels for any Component.