Data Privacy Addendum

This Data Privacy Addendum ("**DPA**") relates to the processing by HackEDU, Inc., d/b/a Security Journey, a Delaware Corporation ("**Provider**") of Personal Data (as defined below) provided by the company or entity that is party ("**Customer**") to the applicable subscription or license agreement and ordering documentation between Customer and Provider (collectively, the "**Agreement**") governing Customer's use of Provider's software and/or hosted service products. This DPA is incorporated into and forms part of, and is subject to the terms and conditions of, the Agreement. If an Affiliate of Customer has executed an Order Form with Provider but is not the original signatory to the Agreement, this DPA is an addendum to and forms part of such Order Form. As used in this DPA, any capitalized terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

1. Definitions

"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data, or has any other meaning given in any Data Protection Laws and Regulations.

"**Data Protection Laws and Regulations**" means any and all data protection and privacy laws throughout the world to the extent they apply to the subject matter of this Agreement, which may include: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons in the European Economic Area ("**EEA**"), which includes the 27 member states of the European Union ("**EU**"), Iceland, Norway, and Liechtenstein, with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, known as the General Data Protection Regulation ("**EU GDPR**"); (ii) United Kingdom General Data Protection Regulation, tailored by the Data Protection Act 2018, as it forms part of the law of England and Wales, Scotland and Northern Ireland, by virtue of Section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) New Swiss Act on Federal Data Protection; (iv) California Consumer Privacy Act of 2018 (the "**CCPA**"), (v) the California Privacy Rights Acts ("CPRA"), (vi) Colorado Privacy Act (the "**CPA**"); (vii) Connecticut Personal Data Privacy Act (the "**CTDPA**"); (vii) Utah Consumer Privacy Act ("**UCPA**"); (viii) Virginia Consumer Data Protection Act (the "**VCDPA**"); and (ix) any other similar data protection laws in any other applicable territory, each as amended, replaced, or superseded.

"**Data Subject**" means the individual to whom the Personal Data relates, and includes equivalent terms under Data Protection Laws and Regulations, such as the term "consumer" as defined in the CCPA, CPA, CTDPA, UCPA, and VCDPA (the "**State Privacy Laws**").

"**Personal Data**" means any information relating to an identified or identifiable natural person or that is otherwise defined as "personal data" or "personal information" (or any analogous concept) under applicable Data Protection Laws and Regulations that is: (i) Processed by Provider's products that are provided as a hosted, software-as-a-service application; (ii) provided to Provider by Customer through the Provider website or in the form of a database or file generated by Provider products that are used in connection with support activities; or (iii) obtained by Provider personnel in the performance of professional services ((i) through (iii) hereunder collectively referred to as "**Services**").

"**Processing (or Process or Processed)**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recordation, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller, or has any other meaning given in any Data Protection Laws and Regulations.

"**SCCs (2021)**" means the agreement incorporated herein by reference pursuant to the European Commission's decision of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

"**Standard Contractual Clauses**" means, collectively, the SCCs (2021), the UK Addendum, and the Swiss Addendum.

"**Subprocessor**" means any Processor engaged by Provider to Process Personal Data, or has any other meaning given in any Data Protection Laws and Regulations.

"**UK Addendum**" means the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner's Office (ICO) and laid before Parliament in accordance with s119A of the United Kingdom's Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.

"**Swiss Addendum**" means the adaptations and supplements to the SCCs (2021) mandated by the Federal Data Protection and Information Commissioner in Switzerland.

2. Processing of Personal Data

2.1 *Provision of Service*. Provider provides a Service to Customer as specified in the Agreement. In connection with this Service, the parties anticipate that Provider may Process Personal Data relating to Data Subjects on behalf of the Customer.

2.2 *The parties' roles*. The parties agree that with regard to the Processing of Personal Data, Customer is the Controller, Provider is the Processor, and Provider may engage Subprocessors pursuant to the requirements of this DPA.

2.3 *Customer's Instructions*. Provider will only Process Personal Data for the performance of the Services pursuant to the Agreement and in accordance with Customer's documented instructions as reasonably contemplated by the Agreement. This DPA, the Agreement, and Customer's use of the Service's features and functionality, are Customer's complete set of instructions to Provider in relation to the processing of Personal Data.

2.4 *Scope of Processing*. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Exhibits 1, 2, and 3 to this DPA.

2.5 *Nature of Customer Data*. Customer represents and warrants that it will not transmit or expose to Provider any (i) protected health information (as that term is used in the Health Insurance Portability and Accountability Act of 1996 (HIPAA)); (ii) cardholder data (as regulated by the Payment Card Industry Security Standards Council); or (iii) sensitive Personal Data (as that term is used in the EU GDPR and UK GDPR) as a part of using the Products, in connection with Support Services, or otherwise under this Agreement.

2.6 *State Privacy Laws*. To the extent that the State Privacy Laws are applicable to the Parties, the Parties agree to the following: (i) Provider is a Service Provider (as defined in the State Privacy Laws) for purposes of the Agreement and this DPA; (ii) Provider shall not retain, use, or disclose Personal Data for any purpose other than for the specific purposes of performing the Services and as set forth in the Agreement or as otherwise permitted by the State Privacy Laws, as applicable; (iii) Provider shall not sell (as defined in the State Privacy Laws, as applicable) Personal Data provided by Customer or processed on Customer's behalf; (iv) Customer is responsible for verifying a consumer request with respect to Personal Data processed by Provider before requesting applicable information from Provider; and (v) Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the State Privacy Laws, as applicable. Provider shall notify Customer if it determines that it cannot meet its obligations under the State Privacy Laws, as applicable. Upon receipt of written notice from Customer that Provider has Processed Personal Data without authorization, Provider will stop and remediate any such Processing.

3. Responsibilities

3.1 *Provider's responsibility*. Provider shall cooperate and provide Customer with assistance that Customer deems reasonably necessary to comply with applicable Data Protection Laws and Regulations with regard to Provider's Processing of Personal Data. Customer acknowledges that Provider is not responsible for determining the requirements of Data Protection Laws and Regulations applicable to Customer's business.

3.2 *Transfers of Personal Data Outside the EU, EEA, UK, and Switzerland.* The Standard Contractual Clauses will apply as follows:

(a) Subject to Exhibit 1, the SCCs (2021) shall apply to the extent: (i) Customer is subject to the Data Protection Laws and Regulations in the EU or EEA; (ii) Personal Data is transferred, either directly or via onward transfer, from the EU and EEA to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the Data Protection Laws and Regulations); and (iii) an alternative legal mechanism of ensuring an adequate level of protection for Personal Data is not available with respect to such transfer(s) as set forth herein.

(b) Where applicable, the parties agree that data transfers from the UK abroad are made pursuant to the UK Addendum, set forth in Exhibit 2, which will apply in the following manner:
(i) The SCCs (2021), which are incorporated by reference into the UK Addendum, will also apply to transfers from the UK, subject to this Section 3.
(ii) The UK Addendum will be deemed executed between the parties, and the SCCs (2021) will be deemed amended as specified by the UK Addendum in relation to transfers from the UK.

(c) Where applicable, the parties agree that the data transfers from Switzerland abroad are made pursuant to the Swiss Addendum, set forth in Exhibit 3 which will apply in the following manner:
(i) The SCCs (2021), which are incorporated by reference into the Swiss Addendum, will also apply to transfers out of Switzerland, subject to this Section 3.
(ii) The Swiss Addendum will be deemed executed between the parties, and the SCCs (2021) will be deemed amended as specified in the Swiss Addendum in relation to transfers from Switzerland.

(d) The Standard Contractual Clauses will not apply to Personal Data that is not transferred, either directly or via onward transfer, outside the EU, EEA, Switzerland, and the UK, as applicable. For the purpose of the Standard Contractual Clauses and Addenda, Customer and its Affiliates shall be deemed "data exporters."

3.3 *Modifications*. If the Standard Contractual Clauses apply as set forth in Section 3.2 of this DPA and if such Standard Contractual Clauses are later deemed inadequate or are disapplied or replaced by a court, government, or regulatory authority during the term of the Agreement, then the parties will negotiate in good faith to implement an alternative legal mechanism of ensuring an adequate level of protection for Personal Data under applicable Data Protection Laws and Regulations. Notwithstanding anything to the contrary herein, in the event that Provider provides Customer with thirty (30) days' notice (which notice may be provided through support channels, Provider's website, Provider's status notifications that may be subscribed to, or such other reasonable means) that Provider has elected to rely on an alternative adequacy mechanism for the transfer of any Personal Data in connection with the Services, the parties shall use such alternative adequacy mechanism, provided such alternative mechanism is approved by the applicable data processing authorities or otherwise permitted by Data Protection Laws and Regulations. In the event that a change in Data Protection Laws and Regulations occurs during the term of this Agreement such that the Services do not enable compliance with such change, and as a result of such change Provider is unable to alter the Services without undue burden (in Provider's reasonable discretion), then Customer may, as its exclusive remedy, elect to terminate the Agreement and all outstanding subscriptions to Provider's Products without penalty, and receive a refund of any prepaid, unused Fees.

3.4 *Customer's responsibility*. Customer shall be responsible for ensuring that it has, and will continue to have, the right to transfer, or provide access to, Personal Data to Provider for Processing. Customer's instructions for the Processing of Personal Data by Provider shall at all times comply with applicable Data Protection Laws and Regulations and Customer shall ensure that Provider's Processing of Personal Data in accordance with Customer's instructions will not cause Provider to violate any applicable Data Protection Laws and Regulations. In the event Customer becomes aware that provided instructions are in conflict with applicable Data Protection Laws and Regulations, Customer will promptly notify Provider. Customer recognizes that Provider does not have a means to verify (i) the residency of each Data Subject, (ii) the aspects of Personal Data that are provided to Provider by Customer in connection with each request by Customer to Process such Personal Data; nor (iii) the location of third parties that Customer chooses to exchange Personal Data with as part of the intended functionality of the Service). Customer shall be responsible for ensuring that all such Personal Data may be Processed by Provider's Services in compliance with Data Protection Laws and Regulations, and Provider will provide all reasonably necessary information to Customer to allow Customer to make such determination upon Customer's written request. If any authorizations or consents of Data Subjects are required for the Processing of Personal Data by Provider, Customer shall be required to obtain any such consents directly from the Data Subjects.

3.5 *Provider's duty of cooperation*. If applicable Data Protection Laws and Regulations require Customer to conduct an assessment of the privacy impacts of any Processing of Personal Data carried out by Provider ("Data Protection Impact Assessment"), Provider will reasonably cooperate with Customer's conduct of the assessment to the extent applicable to Provider's responsibilities under this DPA and the Agreement. If applicable Data Protection Laws and Regulations require Customer to notify, seek guidance from, or consult with any governmental authority or representative body, concerning Provider's Processing of Personal Data, Provider will reasonably cooperate with Customer in connection with such advisory request or consultation to the extent applicable to Provider's responsibilities under this DPA and the Agreement, and as allowed by Data Protection Laws and Regulations.

3.6 *Data Protection Contact*. Provider may be reached at privacy@securityjourney.com in connection with inquiries related to data privacy and data protection matters.

4. Storage and access to Personal Data

4.1 *Data residency*. With respect to Provider's hosted service, Personal Data shall be processed and stored in the United States and allowed to be accessed by or otherwise Processed by Provider's personnel or the Subprocessors. Provider will notify Customer if the foregoing changes (which notice may be provided through an update to Annex III, Provider's support channels, Provider's website, Provider's status notifications to which Customers may subscribe, or such other reasonable means). In the event that the foregoing countries to which Personal Data may be transferred is changed, the parties agree to cooperate in good faith in meeting any additional regulatory or legal requirements necessary to allow such transfers. Notwithstanding the foregoing, Customer hereby acknowledges and agrees that Personal Data may be stored by Provider or its Subprocessors in the United States for operational purposes.

4.2 *Provider's access to Personal Data*. Provider shall ensure that access to Personal Data is restricted to only those personnel who have a need to know to enable Provider to perform its obligations under the Agreement and this DPA. Provider's personnel engaged in the Processing of Personal Data shall be informed of the confidential nature of the Personal Data, have received appropriate training regarding their responsibilities, and be bound in writing by obligations of confidentiality sufficient to protect Personal Data in accordance with the terms of this DPA.

4.3 *Access by authorities*. To the extent legally permitted, Provider will promptly, and no later than five (5) business days following receipt, notify Customer of (i) any request for access to any Personal Data from any regulatory body or government official, and (ii) any warrant, subpoena, or similar request to Provider regarding any Personal Data. Provider will comply with any legal hold from Customer regarding Personal Data and will provide reasonable support so that Customer can comply with third party requests as required by Data Protection Laws and Regulations if Customer cannot otherwise reasonably obtain such information. Provider will reasonably cooperate with Customer if Customer or its regulators properly request access to Personal Data for any reason in accordance with the Agreement, this DPA, or applicable Data Protection Laws and Regulations.

5. Subprocessors

5.1 *Provider's use of Subprocessors*. By executing this DPA, Customer has given its general written consent and authorization for Provider to engage Subprocessors in connection with the Services. The current list of Subprocessors is set forth in Annex III (which may be updated by Provider from time to time in accordance with Section 5.2 of this DPA). Provider may not transfer Personal Data to any other Subprocessor without providing prior written notice to Customer (which notice may be provided through the Provider website or such other reasonable means).

5.2 *Updates to Annex III*. Provider will notify Customer in advance of any changes to Annex III by updating the list contained therein at least thirty (30) days in advance of any Processing by the Subprocessor ("**Notification**"). If Customer has a reasonable objection that relates to the Subprocessor's Processing of Personal Data, Customer may object to Provider's use of the Subprocessor by notifying Provider in writing at privacy@securityjourney.com, within thirty (30) days of Notification. Provider and Customer will work in good faith to resolve any objections, but ultimately, Provider may choose to: (i) not use the Subprocessor; (ii) use the Subprocessor but take corrective steps requested by Customer; or (iii) use the Subprocessor as originally intended. In the event that Provider opts for (iii), Customer may provide notice of termination of the affected portion of Services to Customer.

5.3 *Onward Transfer of Personal Data*. Any transfer by Provider of Personal Data to a Subprocessor will be governed by a written contract providing that the Subprocessor will process Personal Data in accordance with Provider's instructions as required by Data Protection Laws and Regulations. Provider conducts an annual review

and assessment of its Subprocessors to ensure such Subprocessors have in place proper organizational and technical safeguards to ensure the protection of Personal Data.

5.4 *Liability for Subprocessors*. Provider shall be liable for the performance of its Subprocessors to the same extent Provider would be liable if Processing Personal Data itself.

6. Data Subject's rights

6.1 *Requests and complaints*. To the extent legally permitted, Provider shall promptly notify Customer in writing if Provider receives any request from a Data Subject with respect to Personal Data being Processed. Provider shall not directly respond to any such request, unless authorized and directed to do so by Customer or required by applicable Data Protection Laws and Regulations. Provider shall reasonably cooperate with Customer and may charge Customer a reasonable fee for such cooperation with respect to any action taken relating to such request.

7. Security measures

7.1 *Provider's obligations*. Provider shall provide appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Personal Data, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects. Provider shall, at a minimum, maintain the security of the Service and the Personal Data in accordance with the Agreement and any security documentation or policies made available to Customer.

7.2 *Determination of security requirements.* Customer is responsible for reviewing the information Provider makes available regarding its data security and making an independent determination as to whether Provider's Service meets Customer's requirements and legal obligations, including its obligations under this DPA.

8. Security Incident response and notification

8.1 *Discovery and investigation of a breach*. Provider will notify Customer without undue delay upon becoming aware of an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data Processed by Provider (a "**Personal Data Incident**"). Provider shall make reasonable efforts to identify the cause of a Personal Data Incident and take those steps as Provider deems necessary and reasonable in order to remediate the cause of such Personal Data Incident, to the extent that the remediation is within Provider's reasonable control. The obligations set forth herein shall not apply to incidents that are caused directly or indirectly by either the Customer or its users.

8.2 *Notification format and contents*. Provider shall direct its notice by email to the address provided by Customer in Provider's customer portal. Such notice shall include, if known by Provider: (i) a description of the Personal Data Incident; (ii) the categories and approximate numbers of impacted individuals; (iii) possible consequences of the Personal Data Incident; (iv) corrective actions taken or to be taken by Provider, if any; (v) internal point(s) of contact that Customer may engage for managing or responding to Customer about the Personal Data Incident; and (vi) Provider's data protection designated contact's contact information.

9. Retention, return and deletion of Personal Data

9.1 *Return and deletion of Personal Data upon termination*. When Personal Data is no longer necessary for the purposes set forth in this DPA or at an earlier time as Customer requests in writing, Provider will (i) provide to Customer, in the format and on the media as mutually agreed between the parties, a copy of all or, if specified by Customer, any part of the Personal Data; or (ii) delete all, or if specified by the Customer, any part of the Personal Data in Provider's possession, except for backups and monitoring data which will be deleted per Provider's data retention policy. Any Personal Data that is not immediately deleted, will continue to be protected as set forth in this DPA.

9.2 *Customer's copy of Personal Data*. During the term of the Agreement, Provider will provide Customer with the capability to obtain a copy of its Personal Data. Upon termination or expiry of the Agreement, and upon request, Provider will provide a reasonable opportunity for Customer to obtain a copy of its Personal Data and delete the same. This requirement shall not apply to the extent that Provider retains some or all of the Personal Data it has archived on back-up systems, which Provider shall protect from any further processing except to the extent required by Data Protection Laws and Regulations.

10. Limitation of liability. Each party's liability arising out of or related to this DPA, including its exhibits and attachments, whether in contract, tort or under any other theory of liability, is subject to any limitation of liability as set forth in the Agreement and any reference to such limitation of liability of a party means the aggregate liability of the party under the Agreement and this DPA, including its exhibits and attachments, together.

11. Security reports

11.1 *Security reports*. Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Provider shall promptly provide Customer with information related to Provider's information security safeguards and practices, which may include one or more of the following as Customer may request no more than one per annum: (i) a copy of Provider's then-current SOC 2 Type 2 report; (ii) responses to a reasonable information security-related questionnaire; or (iii) a summary of Provider's operational practices related to data protection and security. For the avoidance of doubt, nothing in this Agreement shall be construed as permitting Customer access to Provider's production or non-production systems, source code, or access to anything that may expose confidential information of other customers of Provider. In the event that the SCCs (2021) are applicable, additional audit rights will be as set forth in Exhibits 1, 2, or 3, respectively.

12. Miscellaneous

12.1 *Order of precedence*. Except as specifically set forth in this DPA, the terms and provisions of the underlying Agreement shall remain unmodified and in full force and effect. In the event of a conflict between the terms and conditions of the Standard Contractual Clauses, Exhibits 1, 2, and 3, the Agreement, and this DPA, the conflict shall be resolved in the following order of precedence: (i) Standard Contractual Clauses, (ii) Exhibits 1, 2, and 3, (iii) this DPA, and (iv) the Agreement.

12.2 *Duration of this DPA*. This DPA shall remain in effect until, and automatically expire upon, deletion of all Personal Data by Provider as described in this DPA.

12.3 *Amendments*. If an amendment to this DPA is required in order to comply with applicable Data Protection Laws and Regulations, both parties will work together in good faith to promptly execute a mutually agreeable amendment to this DPA reflecting the requirements set out by the applicable Data Protection Laws and Regulations.

Exhibit 1
SCCs (2021) ADDENDUM

This SCCs (2021) Addendum ("**SCCs (2021) Addendum**") applies if the SCCs (2021) apply as set forth in the DPA.

1. **Processing Generally.**

a. *Modules.* Customer and Provider acknowledge and agree that only Module 2 (Transfer Controller to Processor) of the SCCs (2021) applies to the Processing described in the DPA.

b. *Instructions.* Customer's complete and final documented instructions for the Processing of Personal Data are as set forth in Section 2.3 of the DPA. Any additional or alternate instructions must be agreed upon in a writing executed by authorized representatives of each party. For the purposes of Clause 8.1(a) of the SCCs (2021), the following are deemed the exclusive instructions by the Customer to Process Personal Data: (i) Processing in accordance with this SCCs (2021) Addendum and the Agreement; and (ii) Customer's use of the Service's features and functionality.

c. *Copies*. In the event that Customer provides a copy of the SCCs (2021) to a Data Subject pursuant to Clause 8.3 of the SCCs (2021), Customer shall redact all business secrets and Confidential Information of Provider, including all measures described in Annex II thereto. Provider acknowledges and agrees that Customer may need to provide a meaningful summary of such redacted information to the Data Subject.

d. *Deletion*. The parties acknowledge and agree that any deletion or return of Personal Data that is described in Clause 8.5 of the SCCs (2021) (and certification of the same) shall be conducted as set forth in Section 9.1 of the DPA and shall be provided by Provider only upon Customer's request.

2. **Onward Transfers.** The parties acknowledge and agree that Customer's documented instructions for disclosure of Personal Data to a third party as described in Clause 8.8 of the SCCs (2021) shall be carried out in accordance with Sections 4 and 5 of the DPA.

3. **Security Audits.** The parties agree that they will use reasonable efforts to satisfy any audit requests or requirements described in Clauses 8.9(c)-(e) of the SCCs (2021) through the processes outlined in Section 11.1 of the DPA. In the event that such processes are unable to satisfy the requirements of Customer, then in addition to any audit rights of Customer set forth in the Agreement, upon written request, Provider will provide to Customer all information reasonably required by Customer from time to time to assess Provider's compliance with the SCCs (2021). Provider shall be permitted to redact information that is reasonably deemed sensitive for external exposure. Upon reasonable advance written request of not less than thirty (30) days, at reasonable intervals not to exceed once every twelve months, and with minimal disruption to the daily business operations of Provider, Provider will allow for and contribute to reasonable audits and inspections conducted by Customer (or Customer's independent third-party auditor, provided they enter into Provider's reasonable non-disclosure agreement), including on-site inspections of Provider's business premises for the purpose of assessing Provider's compliance with the SCCs (2021). Customer shall reimburse Provider for any time expended by Provider in fulfilling any such audits or information requests set forth in this section (other than as set forth in Section 11.1 of the DPA, which shall be at no additional cost to Customer) at Provider's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such audit, Customer and Provider shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Provider. Customer understands that due to the third-party hosting and multi-tenant nature of the Services, Provider cannot grant access to the premises, facilities, or records of any Subprocessor or Provider's production or non-production systems, source code, or anything that could expose confidential information of other customers of Provider.

4. **Subprocessors.** The parties agree to utilize Option 2 set forth in Clause 9(a) of the SCCs (2021). Furthermore, the parties agree that any changes to Subprocessors as described in Clause 9(a) of the SCCs (2021) shall be carried out in accordance with Section 5 of the DPA. The parties agree that the copies of the Subprocessor agreements that may be provided by Provider to Customer pursuant to Clause 9(c) of the SCCs (2021) may have all commercial information, or clauses unrelated to the SCCs (2021) or their equivalent,

removed by Provider beforehand; and, that such copies will be provided by Provider in a manner to be determined in its discretion, and only upon written request by Customer.

5. **Liability.** The parties acknowledge and agree that Section 10 of the DPA expressly applies to Clause 12 of the SCCs (2021).

6. **Termination.** The parties agree that in the event Customer terminates the Agreement and/or an Order Form as described in Clause 16 of the SCCs (2021), Customer shall remain liable for all fees set forth on any outstanding Order Form(s), regardless of whether such fees have been invoiced or are yet payable at the time of such termination.

7. **Governing Law.** The Parties agree that this DPA shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, the DPA shall be governed by the law of another EU Member State that does allow for third party beneficiary rights. The parties agree that such EU Member State shall be the Republic of Ireland.

8. **Conflict.** Except as specifically set forth in this Exhibit 1, the terms and provisions of the underlying Agreement shall remain unmodified and in full force and effect. In the event of a conflict between the terms and conditions of the SCCs (2021), the Agreement, this SCCs (2021) Addendum, and any other previously executed data protection or data privacy agreement ("**DPA**"), the conflict shall be resolved in the following order of precedence: (i) SCCs (2021), (ii) this Exhibit 1, (iii) the DPA, and (iv) the Agreement.

9. **Annex I.** The parties acknowledge and agree that Annex I attached hereto shall apply for purposes of the Annex I referenced in the SCCs (2021).

10. **Annex II.** The parties acknowledge and agree that Annex II attached hereto shall apply for purposes of the Annex II referenced in the SCCs (2021).

11. **Annex III.** The parties acknowledge and agree that Annex III attached hereto shall be governed by section 5.2 of the DPA and shall apply for the purposes of the Annex III referenced in the SCCs (2021).

Annex I

A. LIST OF PARTIES

Data exporter(s): Customer (as defined in the Agreement)

Name: ……

Address:
……

Contact person's name, position and contact details: ……

Activities relevant to the data transferred under these Clauses: see below

Signature and date: ……

Role (controller/processor): controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contactperson with responsibility for data protection]*

Role (controller/processor): Processor

Name: HackEDU, Inc., d/b/a Security Journey

Contact person's name, position and contact details: Joe Ferrara, CEO, joe_ferrara@securityjourney.com

Activities relevant to the data transferred under these Clauses: Personal Data will be processed in connection with the use of the Services.

Signature and date: _____

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of data subjects:

- Employees, agents, advisors, freelancers of data exporter (who are natural persons)
- Data exporter's Users authorized by data exporter to use the Services

Categories of personal data transferred

Personal Data submitted by, sent to, or received by the data exporter and its Users in connection with the Services may include, but not be limited to, the name, email address, and IP address related to an individual, manager, team, or in connection with a location or a division of data exporter, for example.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Not applicable.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The Personal Data is transferred on a continued basis.

Nature of the processing

The nature of the Processing is the performance of the Services pursuant to the Agreement, including processing for authentication and training tracking and reporting.

Purpose(s) of the data transfer and further processing

The purpose of the Processing is the performance of the Services pursuant to the Agreement, any Order Form and to the extent further specified by the data exporter in connection with the use of the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal Data will be retained by the data importer in accordance with its data retention policy and used no longer than necessary for the purposes set forth in the Agreement, or until such earlier time as the data exporter requests in writing.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The subject matter, nature and duration of the processing are the performance of the Services pursuant to the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

The supervisory authority with responsibility for ensuring data exporter's compliance with Regulation (EU) 2016/679 shall act as competent supervisory authority.

Annex II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Examples of possible measures:	Description:
Measures of pseudonymisation and encryption of personal data	UUIDs are used in place of plain PII throughout multiple points of data storage. Data is encrypted at-rest utilizing 256-bit Advanced Encryption Standard (AES-256). Data in-transit transferred via encrypted TLS connections.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Access to physical servers is restricted to only authorized personnel. Access events are logged and reviewed. Strong password policies are in place alongside MFA requirements for privileged accounts. Access and permission sets are based on role-based need following the concept of least-privilege. Platform is architected to be fault-tolerant and supported by geographically dispersed infrastructure. Regular automated backups of datastore.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Platform is architected to be fault-tolerant and supported by geographically dispersed infrastructure. Regular automated backups of datastore. Data centers make use of redundant controls and suppliers surrounding physical and environmental controls.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Policies and processes are reviewed at least annually. Policies and processes are exercised on an at-least annual basis to ensure accuracy and effectiveness with deployed technologies. Continual improvement processes exist to ensure controls and measures are effective and accurate to technological and other requirements.
Measures for user identification and authorisation	Platform supports username and password-based authentication controls in addition to supporting Single Sign-on (SSO) functionality for accessing the platform. Verification steps during data access requests are implemented.
Measures for the protection of data during transmission	Data in-transit is transferred via encrypted TLS connections. Firewalls or equivalent controls are implemented to control the flow of network traffic within the platform or to/from the platform.
Measures for the protection of data during storage	Data is encrypted at-rest utilizing 256-bit Advanced Encryption Standard (AES-256). Access to the data storage environment is controlled based on role-based business need following the concept of least-privilege access. Data access events are monitored and logged. Physical controls are implemented to limit, control, and monitor access to the data center environment.
Measures for ensuring physical security of locations at which personal data are processed	Data center access is limited to only approved individuals alongside valid business justification. Access is logged, monitored, and reviewed. Environmental controls are maintained and monitored.

Measures for ensuring events logging	Logging controls are implemented across multiple layers of the platform and supporting infrastructure environments following policy directives. Logging controls and processes are reviewed at-least annually and updated based on changes to requirements or deployed technologies.
Measures for ensuring system configuration, including default configuration	Infrastructure and baseline configuration controls are subject to review and approval requirements. Templated “Infrastructure-as-Code” controls exist where infrastructure and system configurations are defined within code. Changes to systems and infrastructure is subject to review and approval.
Measures for internal IT and IT security governance and management	Dedicated IT and Security personnel are responsible for the day-to-day management of respective programs. Policies and processes governing both programs are reviewed and approved by management at-least annually. As-needed changes and approval conducted as-needed based on evolving requirements and technological changes.
Measures for certification/assurance of processes and products	Policies and processes are reviewed and approved at-least annually. As-needed changes and approval conducted as-needed based on evolving requirements and technological changes. Third-party application security assessments are conducted.
Measures for ensuring data minimisation	Required personal data for product functionality has been limited by design. Considerations for data minimization exist during product design and development processes.
Measures for ensuring data quality	User personal data is provided directly by the customer. Customer can add and update user records as needed. Processes are in-place to process data deletion requests in a timely fashion.
Measures for ensuring limited data retention	Processes are in-place to process data deletion requests in a timely fashion once received or as outlined within contractual agreement.
Measures for ensuring accountability	A security program is maintained and supported by dedicated personnel in addition to members of management. Relevant policies and processes have been implemented and are subject to review and management approval. Security and privacy obligations are supported on contractual obligations where reviewed and approved.
Measures for allowing data portability and ensuring erasure**]**	Platform supports export of reporting and data in common formats. Supporting policies and processes for ensuring data erasure are documented and implemented.

ANNEX III

List of authorized Subprocessors

Name of the Subprocessor	Contact information of the Subprocessor (postal address; email address)	Location of the relevant data processing	Nature of services / processing
Stripe	https://www.stripe.com	United States of America	Payment processing
Segment	https://www.segment.com	United States of America	Analytics and usage
Google	https://www.google.com	United States of America	Analytics and usage
Datadog	https://www.datadog.com	United States of America	Logging tool
Hotjar	https://www.hotjar.com	United States of America	Analytics and usage
Intercom	https://www.intercom.com	United States of America	Communication/support
LinkedIn	https://www.linkedin.com	United States of America	Marketing
Sentry	https://www.sentry.com	United States of America	Debug tooling
Amazon Web Services (AWS)	https://www.aws.com	United States of America	Host
Slack	https://www.slack.com	United States of America	Communication/support
LaunchDarkly	https://www.launchdarkly.com	United States of America	Feature Management
Hubspot	https://www.hubspot.com	United States of America	Communication/Automation
Heroku	https://www.heroku.com	United States of America	Host
Mailer Send	https://www.mailersend.com	United States of America	Communication/support

Exhibit 2
UK Addendum to the SCCs (2021)

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	Date of last signature to this DPA	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Party details from Annex 1 of the EU Standard Contractual Clauses, to which this Exhibit is attached, are incorporated herein.	Party details from Annex 1 of the EU Standard Contractual Clauses, to which this Exhibit is attached, are incorporated herein.
Key Contact	Key contact details from Annex 1 of the EU Standard Contractual Clauses, to which this Exhibit is attached, are incorporated herein.	Key contact details from Annex 1 of the EU Standard Contractual Clauses, to which this Exhibit is attached, are incorporated herein.
Signature (if required for the purposes of Section 2)	Signatures on the DPA are acceptable for this purpose.	Signatures on the DPA are acceptable for this purpose.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or ☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	X	N/A	N/A	General Authorization	Thirty (30) days	N/A
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As set forth in Annex 1 of the SCCs (2021)
Annex 1B: Description of Transfer: As set forth in Annex 1 of the SCCs (2021)
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set forth in Annex 2 of the SCCs (2021)
Annex III: List of Sub processors (Modules 2 and 3 only): As governed by Section 5.2 of the DPA and set forth in Annex III of the SCCs (2021)

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties

and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679"; "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)"; and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union"; "Union"; "EU"; "EU Member State"; "Member State"; and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes" will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Exhibit 3
Swiss Addendum to the SCCs (2021)
This Exhibit 3 to the DPA incorporates by reference the SCCs, the SCCs (2021) Addendum, and the annexes thereof, except that:

1. All references to Regulation (EU) 2016/79 of the European Parliament and of the Council of 27 April 201 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data must be understood and interpreted as references to the Swiss Data Protection Act in the context of data transfers abroad that are subject to the Data Protection Act;

2. Any reference to a supervisory authority shall refer to the Swiss Federal Data Protection and Information Commissioner; and

3. With regard to Clauses 17 and 18, these clauses shall be governed by the law of Switzerland and the Participating Entities agree to the jurisdictions of the courts of Switzerland with regard to any disputes that arise from the clauses in the Swiss Addendum to the SCCs.