

SERVICES AGREEMENT BETWEEN
THE SCHOOL BOARD OF CITRUS COUNTY, FLORIDA
AND
THE ESCAL INSTITUTE OF ADVANCED TECHNOLOGY, INC. /DBA SANS
INSTITUTE
FOR ONLINE EDUCATION SERVICES

THIS AGREEMENT ("Agreement") is entered into by and between The School Board of Citrus County, Florida, a political subdivision of the State of Florida, and a body corporate pursuant to §1001.40, Florida Statutes, whose address is 1007 W. Main Street, Inverness, Florida 34450, hereinafter referred to as "CCSB" or "School Board" and, The Escal Institute of Advanced Technologies, Inc. /dba SANS Institute, a Delaware Corporation whose principal address is 11200 Rockville Pike, Suite 200, North Bethesda, MD 20852, hereinafter referred to as "Contractor" or "Provider" (each a "Party" and collectively referred to as the "Parties").

WHEREAS, CCSB is interested in utilizing the Contractor's software license, hosting, implementation, and training services for Enduser Security Awareness Training Licenses, Engagement Materials Pack, and Phishing Licenses; and

WHEREAS, Florida Administrative Code 6A-1.0102(14) authorizes district school boards to acquire information technology as defined in Florida Statute §282.0041(14) by direct negotiation and contract with the Contractor as best fits the needs of the school district as determined by the district school board; and

WHEREAS, Contractor desires to provide their software license, hosting, implementation, and training services for the Citrus County School District.

NOW, THEREFORE, in consideration of the premises and of the mutual covenants contained herein and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

- 1. Incorporation of Recitals.** The forgoing recitals (WHEREAS CLAUSES) are true and correct and are incorporated herein by reference.

2. **Terms of Agreement.** The term of this Agreement shall commence on November 1, 2023 and continue until October 31, 2024. Notwithstanding any other termination referenced herein or attached hereto, the School Board reserves the right to terminate this Agreement within 30 days prior to the start of each fiscal year (July 1) during the term of this Agreement without cause or subject to any penalties or additional obligations.

3. **Statement of Work.** The Contractor shall provide software license, hosting, implementation, and training services (“Products” and “Services”) as outlined in Attachment B, SANS Institute – Security Awareness Price Quote 00059471, which is incorporated in the Agreement by reference. Additional services and products may be offered through separate statements of work or proposals, all of which are subject to the terms and conditions of this Agreement and all Exhibits. In the event of a conflict of interest between the terms and conditions of this Agreement and any exhibits or attachments, the terms and conditions of this Agreement shall prevail, and the following order of precedence shall be observed:
 - 3.1. This Service Agreement.
 - 3.2. Attachment A – Student Data Privacy Agreement.
 - 3.3. Attachment B – SANS Institute – Security Awareness Price Quote 00059471
 - 3.4. Attachment C – Terms of Service
 - 3.5. Attachment D – Privacy Policy

4. **Payment & Compensation.** The Contractor shall provide services in accordance with Attachment B, SANS Institute – Security Awareness Price Quote 000594 at the rate specified therein. The total compensation under this Agreement shall not exceed **THIRTEEN THOUSAND EIGHT HUNDRED SEVENTY-FIVE AND 00/100 DOLLARS (\$13,875.00)**. Payment will be made in accordance with Section 218.70, Florida Statutes, et. seq., the Local Government Prompt Payment Act.

5. **CCSB Administrator.** The CCSB Administrator assigned to act on behalf of CCSB in all matters pertaining to this Agreement and to authorize services, accept and approve all reports, drafts, products or invoices is **Lance Fletcher, Coordinator of Educational Technology**.

6. **Background Screening:** In the event the requirements include the need for Contractor to visit schools with students present, Contractor agrees to comply with all requirements of Sections 1012.32 and 1012.465, Florida Statutes, and all of its personnel who (1) are to be permitted access to school grounds when students are present, (2) will have direct contact with students, or (3) have access or control of school funds, will successfully complete the background screening required by the

referenced statutes and meet the standards established by the statutes. This background screening will be conducted by CCSB in advance of Contractor or its personnel providing any services under the conditions described in the previous sentence. Contractor shall bear the cost of acquiring the background screening required by Section 1012.32, Florida Statutes, and any fee imposed by the Florida Department of Law Enforcement to maintain the fingerprints provided with respect to Contractor and its personnel. The Parties agree that the failure of Contractor to perform any of the duties described in this section shall constitute a material breach of this Agreement entitling CCSB to terminate this Agreement immediately with no further responsibilities or duties to perform under this Agreement. Contractor agrees to indemnify and hold harmless CCSB, its officers and employees resulting from liability or claims made by any person who may suffer physical or mental injury, death or property damage resulting in the Contractor's failure to comply with the requirements of this Section or with Sections 1012.32 and 1012.465, Florida Statutes.

- 7. Child Neglect.** The Contractor and its employees shall be subject to the requirements of §39.201, Florida Statute that requires the reporting of child abuse or child neglect to the State of Florida, Department of Children and Families via the Florida Abuse Hotline: 1-800-962-2873.
- 8. Indemnification.** The Contractor agrees to indemnify, hold harmless and defend CCSB, its officers, employees, agents and representatives from any and all claims, judgments, costs, and expenses including, but not limited to, reasonable attorney's fees, reasonable investigative and discovery costs, court costs and all other sums which CCSB, its officers, employees, agents and representatives may pay or become obligated to pay on account of any, all and every claim or demand, or assertion of liability, or any claim or action founded thereon, arising or alleged to have arisen out of the products, goods or services furnished by the Contractor, its agents, servants or employees; the equipment of the Contractor, its agents, servants or employees while such equipment is on premises owned or controlled by CCSB; or the negligence of the Contractor or the negligence of the Contractor's agents when acting within the scope of their employment, whether such claims, judgments, costs and expenses be for damages, damage to property including CCSB's property, and injury or death of any person whether employed by the Contractor, CCSB or otherwise.
- 9. Insurance.** Prior to commencement of this Agreement, Contractor(s) and subcontractors will provide a certificate(s) evidencing such insurance coverage to the extent applicable, subject to approval by Risk Management, which shall be attached hereto as Attachment B. Neither approval nor failure to disapprove insurance furnished by the Contractor shall relieve the Contractor from the responsibility to provide insurance as required by this Agreement.

Contractors shall carry and maintain insurance coverage as identified in and the table below. All required insurance must be from insurance carriers that have a rating of "A" or better and a financial size category of "VII" or higher, according to the A. M. Best Company. Notice shall be provided to MCSB at least thirty (30) days in advance of any material change in coverage or cancellation, except as provided for herein.

Except as otherwise specifically authorized in this Agreement, no deductible or self-insured retention for any required insurance provided by the Contractor pursuant to this Agreement will be allowed. To the extent any required insurance is subject to any deductible or self-insured retention (whether with or without approval of MCSB), the Contractor shall be responsible for paying on behalf of MCSB (and any other person or organization that the Contractor has, in this Agreement, agreed to include as an insured for the required insurance) any such deductible or self-insured retention.

The Contractor shall continue to maintain products/completed operations coverage in the amounts stated above for a period of three (3) years after the final completion of the Work.

Compliance with the insurance requirements provided by this section shall not limit the liability of the Contractor, its subcontractors, sub-subcontractors, employees or agents. Any remedy provided to MCSB or MCSB's board members, officers or employees by the insurance provided by the Contractor shall be in addition to and not in lieu of any other remedy (including, but not limited to, as an indemnitee of the Contractor) available to MCSB under this Agreement or as otherwise provided by law.

To the extent identified on the table below, the following provisions shall apply to all insurance coverage required by this section:

- Commercial General Liability Insurance: Coverage shall be provided, with minimum policies limits as set forth in the table below.
- Product Liability and/or Completed Operations Insurance: All Contractors engaging in construction-related activities, as defined by 440.02(8) Florida Statutes, on behalf of MCSB are required to carry this insurance to the limit listed below. All non-construction Contractors whose work for MCSB includes products or services, and the value of these products or services in excess of \$25,000 are required to carry this insurance to the limit listed below.
- Automotive Liability: Any Contractor or vendor transporting district employees, delivering, or transporting district owned equipment or property, or providing services or equipment where a reasonable person would believe MCSB is

responsible for the work of the Contractor from portal to portal is required to carry this insurance to the limit listed below.

- **Workers' Compensation/Employer's Liability:** All non-construction Contractors and vendors that have one or more employees or subcontracts any portion of their work to another individual or company are required to have workers' compensation insurance. For contracts of \$25,000 or more, no State of Florida, Division of Workers' Compensation, Exemption forms will be accepted. All Contractors engaging in construction-related activities, as defined by 440.02(8) Florida Statutes, on behalf of MCSB are required to have workers' compensation insurance. All entities and individuals required to have workers compensation insurance must purchase a commercial workers' compensation insurance policy to the limits listed below. The Workers' Compensation policy must be endorsed to waive the insurer's right to subrogate against MCSB, and its board members, officers and employees in the manner which would result from the attachment of the NCCI Waiver Of Our Right To Recover From Others Endorsement (Advisory Form WC 00 03 13)
- **Professional Liability Insurance (Errors and Omissions):** Contractors providing professional services including but not limited to architects, engineers, attorneys, auditors, accountants, etc. are required to have this insurance to the limits listed below. Professional Liability coverage must be maintained in the amounts stated above for a two-year period following completion of the contract.
- **Cyber Liability and Data Storage:** Contractors or vendors providing software shall provide proof of insurance reflecting, at a minimum, coverage for: Data Loss and System Damage Liability; Security Liability; Privacy Liability; Privacy/Security Breach Response Coverage, including Notification Expenses. Such Cyber Liability coverage must be provided on an Occurrence Form or, if on a Claims Made Form, the retroactive date must be no later than the first date of the Agreement and such claims-made coverage must respond to all claims reported within three (3) years following the period for which coverage is required and which would have been covered had the coverage been on an occurrence basis.

Required Insurance Coverage (check all that apply):

<input type="checkbox"/>	1.	Commercial General Liability Insurance:	
		Bodily Injury and Property Damage Per Occurrence	\$1,000,000
		General Aggregate	\$2,000,000
<input type="checkbox"/>	2.	Product Liability and/or Completed Operations Insurance:	
		Bodily Injury and Property Damage Per Occurrence	\$1,000,000
		General Aggregate	\$2,000,000

<input type="checkbox"/>	3.	Automotive Liability:	
		Bodily Injury and Property Damage: Combined Single Limit (each accident)	\$1,000,000
<input type="checkbox"/>	4.	Workers' Compensation/Employer's Liability:	
		W.C. Limit Required*	Statutory Limits
		E.L. Each Accident	\$500,000
		E.L. Disease – Each Employee	\$500,000
		E.L. Disease – Policy Limit	\$500,000
<input checked="" type="checkbox"/>	5.	Professional Liability Insurance (Errors and Omissions):	
		For services, goods or projects that will exceed \$1,000,000 in values over a year.	
		Each Claim	\$1,000,000
		Annual Aggregate	\$2,000,000
<input checked="" type="checkbox"/>	6.	Cyber Liability and Data Storage:	
		Each Claim	\$1,000,000
		Annual Aggregate	\$1,000,000

10. No Waiver of Sovereign Immunity. Nothing herein is intended to serve as a waiver of sovereign immunity by any agency or political subdivision to which sovereign immunity may be applicable.

11. No Third-Party Beneficiaries. The Parties expressly acknowledge that it is not their intent to create or confer any rights to or obligations upon any third person or entity under this Agreement. None of the Parties intend to directly or substantially benefit a third party by this Agreement. The Parties agree that there are no third-party beneficiaries to this Agreement and that no third party shall be entitled to assert a claim against any of the Parties based upon this Agreement. Nothing herein shall be construed as consent by an agency or political subdivision of the State of Florida to be sued by third Parties for any matter arising out of this or any other contract.

12. Access to and Retention of Documentation. The CCSB, the United States Department of Education, the Comptroller General of the United States, the Florida Department of Education or any of their duly authorized representatives shall have access to any books, documents, papers, and records of the Contractor which are directly pertinent to work and services to be performed under this Agreement for the purpose of audit, examination, excerpting and transcribing. The Parties will retain all such required records, and records required under any state or federal rules, regulations or laws respecting audit, for a period of four years after the CCSB has made final payment and all services have been performed under this Agreement.

13. Contractor's Public Records. Public Records Act/Chapter 119 Requirements. Contractor agrees to comply with the Florida Public Records Act (Chapter 119, Florida Statutes) to the fullest extent applicable, and shall, if this engagement is one for which services are provided, by doing the following:

- 13.1. Contractor and its subcontractors shall keep and maintain public records required by the CCSB to perform the service.
- 13.2. Contractor and its subcontractors shall upon request from the CCSB's custodian of public records, provide the CCSB with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed that provided in chapter 119, Florida Statutes or as otherwise provided by law;
- 13.3. Contractor and its subcontractors shall ensure that public records that are exempt or that are confidential and exempt from the public records disclosure requirements are not disclosed except as authorized by law for the duration of the contract term and following completion of the contract if the Contractor does not transfer the records to the CCSB;
- 13.4. Contractor and its subcontractors upon completion of the contract shall transfer to the CCSB, at no cost, all public records in possession of the Contractor and its subcontractors or keep and maintain the public records required by the CCSB to perform the service. If the Contractor and its subcontractors transfer all public records to the CCSB upon completion of the contract, the Contractor and its subcontractors shall destroy any duplicate public records that are exempt or that are confidential and exempt from the public records disclosure requirements. If the Contractor and its subcontractors keep and maintain public records, upon completion of the contract, the Contractor and its subcontractors shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the CCSB, upon request from the CCSB's custodian of public records, in a format that is compatible with the information technology systems of the CCSB.
- 13.5. The Parties agree that if the Contractor and its subcontractors fail to comply with a public records request, then the CCSB must enforce the Agreement provisions in accordance with the Agreement and as required by Section 119.0701, Florida Statutes.
- 13.6. The failure of the Contractor to comply with the provisions set forth herein shall constitute a default and material breach of this Agreement, which may result in immediate termination, with no penalty to CCSB.

13.7. IF CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THE AGREEMENT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS, THE PUBLIC INFORMATION AND COMMUNICATIONS OFFICER, EMAIL ADDRESS: BLAIRL@CITRUSSCHOOLS.ORG AND PUBLICRECORDS@CITRUSSCHOOLS.ORG; TELEPHONE NUMBER: 352-726-1931 ext. 2211, 1007 W. MAIN STREET, INVERNESS, FLORIDA 34450.

14. Non-Discrimination. The Parties shall not discriminate against any employee or participant in the performance of the duties, responsibilities, and obligations under this Agreement because of race, age, religion, color, gender, national origin, marital status, disability or sexual orientation.

15. Termination. This Agreement may be canceled with or without cause by either party during the term hereof upon thirty (30) days written notice to the other party of its desire to terminate this Agreement.

16. Records. Each Party shall maintain its own respective records and documents associated with this Agreement in accordance with the records retention requirements applicable to public records. Each party shall be responsible for compliance with any public documents request served upon it pursuant to Section 119.07, Florida Statutes, and any resultant award of attorney's fees for non-compliance with that law.

17. Entire Agreement. This document incorporates and includes all prior negotiations, correspondence, conversations, Agreements and understandings applicable to the matters contained herein and the Parties agree that there are no commitments, Agreements or understandings concerning the subject matter of this Agreement that are not contained in this document. Accordingly, the Parties agree that no deviation from the terms hereof shall be predicated upon any prior representations or Agreements, whether oral or written.

18. Amendments. No modification, amendment, or alteration in the terms or conditions contained herein shall be effective unless contained in a written document prepared with the same or similar formality as this Agreement and executed by each party hereto.

19. Preparation of Agreement. The Parties acknowledge that they have sought and obtained competent advice and counsel as was necessary for them to form a full and

complete understanding of all rights and obligations herein and that the preparation of this Agreement has been their joint effort. The language agreed to herein express their mutual intent and the resulting document shall not, solely as a matter of judicial construction, be construed more severely against one of the Parties than the other.

20. Waiver. The Parties agree that each requirement, duty and obligation set forth herein is substantial and important to the formation of this Agreement and, therefore, is a material term herein. Any party's failure to enforce any provision of this Agreement shall not be deemed a waiver of such provision or modification of this Agreement. A waiver of any breach of a provision of this Agreement shall not be deemed a waiver of any subsequent breach and shall not be construed to be a modification of the terms of this Agreement.

21. Compliance with Laws. Each party shall comply with all applicable federal and state laws, codes, rules and regulations in performing its duties, responsibilities and obligations pursuant to this Agreement.

22. Law, Jurisdiction, Venue, Waiver of Jury Trial. The Contract Documents shall be interpreted and construed in accordance with and governed by the laws of the State of Florida. The exclusive venue for any lawsuit arising from, related to, or in connection with this Agreement shall be in the state courts of the Fifth Judicial Circuit in and for Citrus County, Florida. If any claim arising from, related to, or in connection with this Agreement must be litigated in federal court, the exclusive venue for any such lawsuit shall be in the United States District Court or United States Bankruptcy Court for the Middle District of Florida. **EACH PARTY HEREBY EXPRESSLY WAIVES ANY RIGHTS IT MAY HAVE TO A TRIAL BY JURY OF ANY CIVIL LITIGATION RELATED TO THIS AGREEMENT.**

23. Binding Effect. This Agreement shall be binding upon and inure to the benefit of the Parties hereto and their respective successors and assigns.

24. Assignment. Neither this Agreement nor any interest herein may be assigned, transferred or encumbered by any party without the prior written consent of the other party. There shall be no partial assignments of this Agreement, including, without limitation, the partial assignment of any right to receive payments from CCSB. This contract may not be assigned by the Contractor in any fashion, whether by operation of law, or by conveyance of any type, including without limitation, transfer of stock in Contractor, without the prior written consent of the CCSB which consent the CCSB may withhold in its sole discretion.

25. Force Majeure. Neither party shall be obligated to perform any duty, requirement or obligation under this Agreement if such performance is prevented by fire, hurricane, earthquake, explosion, wars, sabotage, accident, flood, acts of God, strikes, or other

of this Agreement, nor in any way affect this Agreement and shall not be construed to create a conflict with the provisions of this Agreement.

29. Authority. Each person signing this Agreement on behalf of either party individually warrants that he or she has full legal authority to execute this Agreement on behalf of the party for whom he or she is signing and to bind and obligate such party with respect to all provisions contained in this Agreement.

30. Excess Funds. Any party receiving funds paid by CCSB under this Agreement agrees to promptly notify CCSB of any funds erroneously received from CCSB upon the discovery of such erroneous payment or overpayment. Any such excess funds shall be refunded to CCSB with interest calculated from the date of the erroneous payment or overpayment. Interest shall be calculated using the interest rate for judgments under Section 55.03, Florida Statutes, applicable at the time the erroneous payment or overpayment was made by CCSB.

31. Independent Contractor. The Contractor certifies that it is an independent Contractor and shall not employ, contract with, or otherwise use the services of any officer or employee of CCSB. The Contractor certifies that its owner(s), officers, directors or agents, or members of their immediate family, do not have an employee relationship or other material interest with the CCSB.

32. Conduct While on School Property. The Contractor acknowledges that its employees and agents will behave in an appropriate manner while on the premises of any school facility and shall at all times conduct themselves in a manner consistent with CCSB policies and within the discretion of the premises administrator (or designee). It is a breach of this Agreement for any agent or employee of the Contractor to behave in a manner which is inconsistent with good conduct or decorum or to behave in any manner that will disrupt the educational program or constitute any level of threat to the safety, health, and wellbeing of any student or employee of the CCSB. The Contractor agrees to immediately remove any agent or employee if directed to do so by the premises administrator or designee.

33. Discriminatory Vendor and Scrutinized Companies Lists; Countries of Concern. Contractor represents that it has not been placed on the “discriminatory vendor list” as provided in Section 287.134, Florida Statutes, and that it is not a “scrutinized company” pursuant to Sections 215.473 or 215.4725, Florida Statutes. Contractor represents and certifies that it is not, and for the duration of the Term will not be, ineligible to contract with the School Board on the grounds stated in Section 287.135, Florida Statutes. Contractor represents that it is, and for the duration of the term of this Agreement will remain, in compliance with Section 286.101, Florida Statutes.

34. Prohibited Telecommunications Equipment. Contractor represents and certifies that Contractor and all subcontractors do not use any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, as such terms are used in 48 CFR §§ 52.204-24 through 52.204-26. Contractor represents and certifies that Contractor and all subcontractors shall not provide or use such covered telecommunications equipment, system, or services during the term of this Agreement.

35. Public Entity Crime Act. Contractor represents that it is familiar with the requirements and prohibitions under the Public Entity Crime Act, Section 287.133, Florida Statutes, and represents that its entry into this Agreement will not violate that Act. Contractor further represents that there has been no determination that it committed a “public entity crime” as defined by Section 287.133, Florida Statutes, and that it has not been formally charged with committing an act defined as a “public entity crime” regardless of the amount of money involved or whether Contractor has been placed on the convicted vendor list.

36. Debarment. By signing this Agreement, Contractor certifies, to the best of its knowledge and belief, that it and its principals:

36.1. Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by a federal department or agency.

36.2. Have not, within the preceding five-year period, been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state or local) transaction or contract under public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements or receiving stolen property.

36.3. Are not presently indicted or otherwise criminally charged by a governmental entity (federal, state or local) with commission of any of the offenses enumerated in the preceding paragraph (b).

36.4. Have not within the preceding five-year period had one or more public transactions (federal, state or local) terminated for cause or default.

36.5. Contractor agrees to notify CCSB within 30 days after the occurrence of any of the events, actions, debarments, proposals, declarations, exclusions,

convictions, judgments, indictments, informations, or terminations as described in subparagraphs 1 through 4 above, with respect to Contractor or its principals.

37. Confidential Student Information. Notwithstanding any provision to the contrary contained in this Agreement between the Contractor and CCSB; Contractor and its officers, employees, agents, representatives, Contractors, and sub-Contractors shall fully comply with the requirements of Sections 1002.22, 1002.221, and 1006.1494 Florida Statutes, or any other law or regulation, either federal or State of Florida, regarding confidentiality of student information and records, Further, Contractor for itself and its officers, employees, agents, representatives, Contractors, or sub-Contractors, shall fully indemnify and hold the CCSB and its officers and employees harmless for any violation of this covenant, including but not limited to defending the CCSB and its officers and employees against any complaint, administrative or judicial proceeding, payment of any penalty imposed upon the CCSB or payment of any and all costs(s), damages (s), judgment(s), or loss(es) incurred by or imposed upon the CCSB arising out of the breach of this covenant by the Contractor, or an officer, employee, agent, representative, Contractor, or sub-Contractor of the Contractor to the extent and only to the extent that the Contractor or an officer, employee, agent, representative, Contractor, or sub-Contractors of the Contractor shall either intentionally or negligently violate the provisions of this covenant, or Sections 1002.22, 1002.221 or 1006.1494, Florida Statutes. This provision shall survive the termination of or completion of all performance or obligations under this Agreement and shall be fully binding upon Contractor until such time as any proceeding brought on account of this covenant is barred by any applicable statute of limitations.

38. Confidentiality of Data/Information Provided. CCSB will allow the Contractor access to limited data/information as identified in the Statement of Work as necessary to perform the Services and pursuant to the terms of this Agreement in compliance with FERPA, COPPA, PPRA, 34 CFR 99.31(b) and Florida Statutes sections 1001.41 and 1002.22 all other privacy statutes as it relates to data privacy and security, as may be amended from time to time, hereinafter interchangeably referred to as confidential information, student data, confidential data, student record information, personal identifiable information ("PII"), or protected information.. The Contractor shall only use the data and information provided by CCSB for the purpose specified in the Statement of Work, and shall not disclose, copy, reproduce or transmit such data/information obtained under this Agreement and/or any portion thereof, except as necessary to fulfill the Agreement or as may be required by law.

39. Protection and Handling of Data.

- 39.1.Data Confidentiality and Security** - Contractor shall implement appropriate measures designed to ensure the confidentiality and security of Protected Information as required in the Student Data Privacy Agreement attached hereto as Attachment A.
- 39.2.Compliance** - Contractor will not knowingly permit any Contractor's personnel to have access to any CCSB facility or any records or data of CCSB if the person has been convicted of a crime in connection with (i) a dishonest act, breach of trust, or money laundering, or has agreed to enter into a pretrial diversion or similar program in connection with a prosecution for such offense, as described in Section 19 of the Federal Deposit Insurance Act, 12 U.S.C. §1829(a); or (ii) a felony. Contractor shall assure that all contracts with subcontractors impose these obligations on the subcontractors and shall monitor the subcontractors' compliance with such obligations. No subcontractors may be used without prior written consent of CCSB.
- 39.3.FERPA** - To the extent services provided hereunder pertain to the access to student information, Contractor shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA) and Sections 1001.41 and 1002.22, Florida Statutes (the Protection of Pupil Privacy Acts), and other applicable laws and regulations as they relate to the release of student information. Notwithstanding the above, it is understood and agreed that CCSB shall obtain any necessary consents from parents or students prior to providing student information to Contractor, and CCSB is wholly responsible for providing annual notice to students and parents of their rights with respect to Florida Statutes.
- 39.4.HIPAA, CIPA, and GLBA** - Contractor also agrees to comply with all applicable state and federal laws and regulations, including Health Information Privacy and Accountability Act (HIPAA), Children Internet Protection Act (CIPA), and the Gramm-Leach Bliley Act (GLBA).
- 39.5.Data De-Identification** - Contractor may use aggregate data only for product development, research, or other purposes expressly permitted by the Family Education Rights Privacy Act (FERPA) and the Student Online Personal Information Protection Act (SOPIPA). Contractor must have approval of the CCSB to publish or market CCSB data.
- 39.6.Data Security** – Contractor agrees to protect and maintain the security of data with protection security measures that include maintaining secure environments that are patched with all appropriate security updates as designated by a relevant authority (e.g. Microsoft notifications, etc.) Likewise, CCSB agrees to conform to the following measures to protect and secure data:

- 39.6.1. Data Transmission.** Contractor agrees that any and all transmission or exchange of system application data with CCSB and/or any other Parties shall take place via secure means, e.g. HTTPS, FTPS, SFTP, or equivalent.
- 39.6.2. Data Storage and Backup.** Contractor agrees that any and all CCSB data will be stored, processed, and maintained solely on designated servers and that no CCSB data at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, unless that storage medium is in use as part of Contractor's designated backup and recovery processes. All servers, storage, backups, and network paths utilized in the delivery of the service shall be contained within the states, districts, and territories of the United States unless specifically agreed to in writing by an CCSB officer with designated data, security, or signature authority. An appropriate officer with the necessary authority can be identified by the CCSB Director of Technology for any general or specific case. Contractor agrees to store all CCSB backup data stored as part of its backup and recovery processes in encrypted form, using no less than 128 bit key.
- 39.6.3. Data Re-Use.** Contractor agrees that any and all data exchanged shall be used expressly and solely for the purposes enumerated in this Agreement. Data shall not be distributed, repurposed, or shared across other applications, environments, or business units of Contractor. As required by Federal law, Contractor further agrees that no CCSB data of any kind shall be revealed, transmitted, exchanged, or otherwise passed to other Contractors or interested Parties except as necessary in order to perform the Services. Any other transmission or exchange of CCSB data is only permitted on a case-by-case basis as specifically agreed to in writing by an CCSB officer with designated data, security, or signature authority.
- 39.6.4. End of Agreement Data Handling.** Contractor will ensure that District Data is encrypted and that all device/medium will be scanned at the completion of any contract or service Agreement and/or research study or project to ensure that no District Data, PII, personal information and/or student record information is stored on such electronic devices/medium. Furthermore, Contractor will have in place a service that will allow Contractor to wipe the hard drive on any stolen laptop or mobile electronic device remotely and have a protocol in place to ensure compliant use by employees.
- 39.6.5.** Contractor agrees that upon termination of this Agreement and requested by CCSB in writing it shall erase, destroy, and render unreadable all CCSB

data, and certify in writing that these actions have been completed within thirty (30) days of the termination of this Agreement or within seven (7) days of the request of an agent of CCSB, whichever shall come first.

39.6.6. If CCSB receives a subpoena, warrant, or other legal order, demand (including an application for public information filed pursuant to Florida public records laws, or request seeking Data maintained by Contractor, the CCSB will promptly provide a copy of the application to Contractor. Contractor will promptly supply CCSB with copies of records or information required in order for the CCSB to respond, and will cooperate with the CCSB's reasonable requests in connection with its response.

39.6.7. Upon receipt of a litigation hold request, Contractor will preserve all documents and CCSB data as identified in such request, and suspend any operations that involve overwriting, or potential destruction of documentation arising from such litigation hold.

39.6.8. Data Breach - Contractor agrees to comply with the Florida Information Protection Act database breach notification process and all applicable laws that require the notification of individuals in the event of unauthorized release of personally identifiable information or other event requiring notification. In the event of a breach of any of Contractor's security obligations or other event requiring notification under applicable law ("Notification Event"), Contractor agrees to notify CCSB immediately and assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless, and defend CCSB and its trustees, officers, and employees from and against any claims, damages, or other harm related to such Notification Event.

39.6.9. Mandatory Disclosure of Protected Information - If Contractor becomes compelled by law or regulation (including securities laws) to disclose any Protected Information, Contractor will provide CCSB with written notice within 72 hours, so that CCSB may seek an appropriate protective order or other remedy. If a remedy acceptable to CCSB is not obtained by the date that Contractor must comply with the request, Contractor will furnish only that portion of the Protected Information that it is legally required to furnish, and Contractor shall require any recipient of the Protected Information to exercise commercially reasonable efforts to keep the Protected Information confidential. As soon as practicable, upon CCSB request, provide CCSB with a copy of its response.

39.6.10. Remedies for Disclosure of Confidential Information – Contractor and CCSB acknowledge that unauthorized disclosure or use of the Protected

Information may irreparably damage CCSB in such a way that adequate compensation could not be obtained from damages in an action at law. Accordingly, the actual or threatened unauthorized disclosure or use of any Protected Information shall give CCSB the right to seek injunctive relief restraining such unauthorized disclosure or use, in addition to any other remedy otherwise available (including reasonable attorneys' fees). Contractor hereby waives the posting of a bond with respect to any action for injunctive relief. Contractor further grants CCSB the right, but not the obligation, to enforce these provisions in Contractor's name against any of Contractor's employees, officers, board members, owners, representatives, agents, Contractors, and subcontractors violating the above provisions.

- 39.6.11. Safekeeping and Security** - As part of the Services, Contractor will be responsible for safekeeping all keys, access codes, combinations, access cards, personal identification numbers, and similar security codes and identifiers issued to Contractor's employees, agents, or subcontractors. Contractor agrees to require its employees to promptly report a lost or stolen access device or information.
- 39.6.12. Non-Disclosure** – Contractor is permitted to disclose Confidential Information to its employees, authorized subcontractors, agents, consultants, and auditors on a need to know basis only, provided that all such subcontractors, agents, consultants, and auditors have written confidentiality obligations to Contractor and CCSB.
- 39.6.13. Request for Additional Protection** - From time to time, CCSB may reasonably request that Contractor protect the confidentiality of certain Protected Information in particular ways to ensure that confidentiality is maintained. Contractor has the right to reasonably decline CCSB's request.
- 39.6.14. Data Ownership-** Unless expressly agreed to the contrary in writing, all CCSB Data or PII prepared by Contractor (or its subcontractors) for the CCSB will not be disclosed to any other person or entity.
- 39.6.15.** Contractor warrants to the CCSB that the CCSB will own all rights, title and interest in any and all intellectual property created in the performance of this Agreement and will have full ownership and beneficial use thereof, free and clear of claims of any nature by any third party including, without limitation, copyright or patent infringement claims. Contractor agrees to assign and hereby assigns all rights, title, and interest in any and all CCSB created intellectual property created in the performance of the Agreement

to the CCSB, and will execute any future assignments or other documents needed for the CCSB to document, register, or otherwise perfect such rights. Notwithstanding the foregoing, Contractor retains all right, title and interest in and to its software, documentation, training and implementation materials and other materials provided in connection with Contractor's services (collectively, "Contractor IP"). Contractor grants to the CCSB a personal, nonexclusive license to use the Contractor IP for its own non-commercial, incidental use as set forth in the end user license Agreement accompanying such software and as contemplated herein. All data of the CCSB remains the property of the CCSB.

39.6.16. It is understood and agreed that the CCSB is the exclusive Owner of the CCSB data and that at no point in time does or will the Contractor become the Owner of any CCSB Data, PII or CCSB files, and that should the Contractor be subject to dissolution or insolvency, CCSB data, PII, or files will not be considered an asset or property of the Contractor. The CCSB reserves the right to demand the prompt return of any and all CCSB data and PII at any time and for any reason whatsoever.

40. Illegal Alien Labor. The Parties shall each comply with all federal and state laws, including but not limited to section 448.095, Florida Statutes, prohibiting the hiring and continued employment of aliens not authorized to work in the United States. The Parties must not knowingly employ unauthorized aliens working under this Agreement and should such violation occur shall be cause for termination of the Agreement. The Parties will utilize the E-verify system established by the U.S. Department of Homeland Security to verify the employment eligibility of its new employees working under this Agreement hired during the contract term, and will further include in all subcontracts for subcontractors performing work or providing services pursuant to this Agreement an express written requirement that the subcontractor utilize the E-Verify system to verify the employment eligibility of all new employees hired by the subcontractor to work under this Agreement during the contract term. The Contractor shall receive and retain an affidavit from the subcontractor stating that the subcontractor does not employ, contract with, or subcontract with an unauthorized alien to work under this Agreement. Contractor's knowing failure to comply with this subsection may result in termination of the Agreement and debarment of the Contractor from all public contracts for a period of no less than one (1) year.

41. FEDERAL GRANTS TERMS AND CONDITIONS. For any Agreement that involves, receives or utilizes Federal Grants funding, the following terms and conditions shall be considered a part of the Agreement and the Contractor accepts and acknowledges that it is and will continue to be in compliance with said terms and conditions for the term of the award:

- 41.1. Recovered Materials (2 CFR §200.322) applies to all contracts greater than \$10,000.** Contractor must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds \$10,000 or the value of the quantity acquired during the preceding fiscal year exceeded \$10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.
- 41.2. Federal Drug Free Workplace.** Contractor agrees to comply with the drug-free workplace requirements for federal Contractors pursuant to 41 U.S.C.A. § 8102.
- 41.3. Byrd Anti-Lobbying Amendment (31 U.S.C. 1352) applies if contract is greater than or equal to \$100,000.** Contractor certifies that it has filed the required certification and that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of an agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Contractor must disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award.
- 41.4. Energy Efficiency / Conservation (42 U.S.C. 6201).** Contractor agrees to comply with the mandatory standards and policies relating to energy efficiency contained in the state energy conservation plan issued in compliance with the Energy Policy and Conservation Act (42 U.S.C. 6201).
- 41.5. Clean Air Act (42 U.S.C. 7401 et seq.) and the Federal Water Pollution Control Act (33 U.S.C. 1251 et seq.), as amended applies to contracts and subgrants in excess of \$150,000.** Contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251-1387). Contractor shall report any and all violations to the Federal awarding agency and the Regional Office of the EPA and notify CCSB concurrently within 30 days of notice of the violation.
- 41.6. Remedies For Violation or Breach of Contract.** Failure of the vendor to provide products within the time specified in the ITB shall result in the following: The Buyer shall notify vendor in writing within five (5) calendar days via the Vendor

Performance Form and provide five (5) calendar days to cure. If awarded vendor cannot provide product, CCSB reserves the right to purchase product from the next lowest responsive and responsible bidder. The defaulting vendor may be responsible for reimbursing CCSB for the price differences.

41.7. Debarment and Suspension. Contractor certifies that it complies fully with the Federal Debarment Certification regarding debarment suspension, ineligibility, and voluntary exclusion, in accordance with 2 CFR part 180 that implement Executive Orders 12549 and 12689. Furthermore, Contractor certifies that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any federal department or agency.

41.8. Equal Employment Opportunity. During the performance of this contract, Contractor agrees as follows:

41.8.1. Contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. Contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the contracting officer setting forth the provisions of this nondiscrimination clause.

41.8.2. Contractor will, in all solicitations or advancements for employees placed by or on behalf of the Contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.

41.8.3. Contractor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to

such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the Contractor's legal duty to furnish information.

- 41.8.4.** Contractor will send to each labor union or representative of workers with which he has a collective bargaining Agreement or other contract or understanding, a Record Retention and access requirements to all records. Contractor will send to each labor union or representative of workers with which he has a collective bargaining Agreement or other contract or understanding, a notice, to be provided by the agency contracting officer, advising the labor union or workers' representative of the Contractor's commitments under Section 202 of Executive Order No. 11246 of September 24, 1965, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.
- 41.8.5.** Contractor will comply with all provisions of Executive Order No. 11246 of Sept. 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.
- 41.8.6.** Contractor will furnish all information and reports required by Executive Order No. 11246 of September 24, 1965, and by the rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the contracting agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.
- 41.8.7.** In the event of the Contractor's noncompliance with the nondiscrimination clauses of this contract or with any of such rules, regulations, or orders, this contract may be cancelled, terminated, or suspended in whole or in part and the Contractor may be declared ineligible for further Government contracts in accordance with procedures authorized in Executive Order No. 11246 of Sept. 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in Executive Order No. 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.
- 41.8.8.** Contractor will include the provisions of paragraphs 39.8 in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to Section 204 of Executive Order No. 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. Contractor will take such action with respect to any subcontract or purchase order as may be directed by the

Secretary of Labor as a means of enforcing such provisions including sanctions for noncompliance: Provided, however, that in the event the Contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction, the Contractor may request the United States to enter into such litigation to protect the interests of the United States.

41.9. Copeland “Anti-Kickback” Act (18 U.S.C. 874 And 40 U.S.C. 276c).

Contractor certifies that it is, and will continue to be, for the term of this contract in for compliance with the Copeland “Anti-Kickback” Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, “Contractors and subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States”). The Act provides that each Contractor or sub recipient must be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The non-Federal entity must report all suspected or reported violations to the Federal awarding agency.

41.10. Davis-Bacon Act, as Amended (40 U.S.C. 276A TO A-7).

Contractor certifies that it is, and will continue for the term of this contract, to be in compliance with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, “Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction”). In accordance with the statute, the Contractor is herein required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor. In addition, Contractor agrees to pay wages not less than once a week. Contractor must provide a copy of the current prevailing wage determination issued by the Department of Labor in each solicitation. Contractor acknowledges that the decision to award this contract or subcontract is conditioned upon the acceptance of the wage determination which the Contractor accepts. Contractor agrees to report all suspected or reported violations to the Federal awarding agency and to notify CCSB concurrently. Contractor certifies that it is, and will continue to be, for the term of this contract in full compliance with the Copeland “Anti-Kickback” Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, “Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States”). The Act provides that each Contractor or sub recipient must be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the

compensation to which he or she is otherwise entitled. The non-Federal entity must report all suspected or reported violations to the Federal awarding agency.

41.11. Contract Work Hours and Safety Standards Act (40 U.S.C. 327-333).

Contractor certifies that it is, and will continue for the term of this contract, to be in compliance with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, each Contractor must be required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

41.12. Health And Safety Standards in Building Trades and Construction Industry (40 U.S.C. 3704). No laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous, or dangerous.

41.13. All website or software terms contained in click-through Agreements in connection with Contractors services are disclaimed by CCSB to the extent the terms are in addition to, conflict or are inconsistent with the terms of this Agreement.

42. Copyrights. The Contractor is hereby notified that the federal awarding agency reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish or otherwise use, and to authorize others to use, for federal government purposes: the copyright in any work developed under a grant, subgrant, or contract under a grant or subgrant; and, any rights of copyright to which a grantee, subgrantee or a Contractor purchases ownership with grant support. Furthermore, the Parties agree that the CCSB has the right to make copies of any materials, whether in tangible or electronic means or media, that are delivered under the provisions of this Agreement for use within the School District for purposes related to CCSB business, operations, the delivery of the educational program or to comply with the requirements of law, rule, policy or regulation. Any material not designated as reproducible by Contractor may not be copied by the CCSB provided that such material was copyrighted by Contractor before performance under this Agreement and was not developed specifically for CCSB under this Agreement.

43. Authority to Execute Agreement. Each person signing this Agreement on behalf of either Party individually warrants that he or she has full legal power to execute this Agreement on behalf of the Party for whom he or she is signing, and to bind and obligate such Party with respect to all provisions contained in this Agreement.

THE PARTIES REPRESENT THAT THEY HAVE THOROUGHLY DISCUSSED ALL ASPECTS OF THE AGREEMENT, ATTACHMENTS, AND EXHIBITS THERETO WITH THEIR RESPECTIVE ATTORNEY(S), THAT THEY FULLY UNDERSTAND ALL OF ITS PROVISIONS, AND THAT THEY ARE VOLUNTARILY ENTERING INTO THE AGREEMENT AND ADDENDUM WITH THE FULL KNOWLEDGE OF ITS LEGAL SIGNIFICANCE AND WITH THE INTENT TO BE LEGALLY BOUND BY ITS TERMS.

IN WITNESS WHEREOF, the Parties hereto have made and executed this Agreement on the date first above written.

The School Board of Citrus County, Florida: [Redacted] Douglas A. Dodd, Chairman Date: <u>10/10/23</u>	The Escal Institute of Advanced Technology, Inc. /dba SANS Institute: [Redacted] By: _____ Title: <u>Contracts Specialist</u> Date: <u>9/14/2023</u>
---	--

Attachments: (list all attachments with the exact title of the document)

Attachment A, Student Data Privacy Agreement

Attachment B, SANS Institute – Security Awareness Price Quote 00059471

Attachment C, Terms and Conditions

Attachment D, Privacy Policy

Contractor Contact Name: Keeton Ellis

Phone Number: 970-209-8313

Email Address: kellis@sans.org

ATTACHMENT A
AGREEMENT BETWEEN
THE SCHOOL BOARD OF CITRUS COUNTY, FLORIDA
AND

The Escal Institute of Advanced Technologies, Inc. /dba SANS Institute

STANDARD STUDENT DATA PRIVACY AGREEMENT

This Student Data Privacy Agreement (“**DPA**”), as developed by the Student Data Privacy Consortium (“**SDPC**”) and as modified by The School Board of Citrus County, Florida, is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between:

The School Board of Citrus County, Florida, located at 1007 W. Main Street, Inverness, Florida 34450 (the “**LEA**”)

and

The Escal Institute of Advanced Technologies, Inc. /dba SANS Institute located at 11200 Rockville Pike, Suite 200, North Bethesda, MD 20852(the “**Provider**”).

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

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

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

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

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions. Check if Required**

If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.

- ✓ If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H"**. (Optional)

If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three (3) years. **Exhibit "E"** will expire three (3) years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**").
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: Lance Fletcher
Title: Coordinator of Educational Technology
Address: 3741 W. Educational Path, Lecanto, FL 34461
Phone: 352-746-3437
Email: fletcherla@citruschools.org

The designated representative for the Provider for this DPA is:

Name: Ashley Sudderth
Title: Director of Governance and Risk
Address: 11200 Rockville Pike, Suite 200, North Bethesda, MD 20852
Phone: 301-654-7267
Email: asudderth@sans.org

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

LEA: The School Board of Citrus County, Florida.

Signature: 

Printed Name: Douglas A. Dodd

Title: Chairman

Date: 10/10/23

Provider: The Escal Institute of Advanced Technologies, Inc. /dba SANS Institute

Signature: 

Printed Name: Suzanne Rosa

Title: Contracts Specialist

Date: 9/14/2023

STANDARD CLAUSES

Version 1.0

Article I. ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

Article II. ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in

a reasonably timely manner (and no later than forty-five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors**. Provider shall enter into written Agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

Article III. ARTICLE III: DUTIES OF LEA

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

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

Article IV. ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit "A"** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality Agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non- public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.
 - (a) **De-Identified Data:** Provider agrees not to attempt to re-identify De-Identified Student Data. De- Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a)

that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented.

5. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a **"Directive for Disposition of Data"** form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ **Exhibit "D"**, no further written request or notice is required on the part of either party prior to the disposition of Student Data described in **Exhibit "D"**.
6. **Advertising Limitations**. Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

Article V. ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits**. No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality Agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably

with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security**. The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and

- iv. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

Article VI. ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as Exhibit "E"), be bound by the terms of Exhibit "E" to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

Article VII. MISCELLANEOUS

1. **Termination**. In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service Agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of

Service, Privacy Policies, or with any other bid/RFP, license Agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between **Exhibit “H”**, the SDPC Standard Clauses, and/or the Supplemental State Terms, **Exhibit “H”** will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire Agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or Agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business In the event that the Provider sells, merges, or

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

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

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

EXHIBIT "A"

DESCRIPTION OF SERVICES

Nature and Purpose of the Processing:

- SANS will process personal data for the purpose of providing the Services as described in Attachment B.
- The Purpose for processing is to allow system access, usage, interaction and authorization data.

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	<input type="checkbox"/>
	Other application technology meta data-Please specify:	<input type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application	<input type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/>
	Observation data	<input type="checkbox"/>
	Other assessment data-Please specify:	<input type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>
Communications	Online communications captured (emails, blog entries)	<input type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/>
Demographics	Date of Birth	<input type="checkbox"/>
	Place of Birth	<input type="checkbox"/>
	Gender	<input type="checkbox"/>
	Ethnicity or race	<input type="checkbox"/>
	Language information (native, or primary language spoken by student)	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Other demographic information-Please specify:	<input type="checkbox"/>
Enrollment	Student school enrollment	<input type="checkbox"/>
	Student grade level	<input type="checkbox"/>
	Homeroom	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input type="checkbox"/>
	Year of graduation	<input type="checkbox"/>
	Other enrollment information-Please specify:	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input type="checkbox"/>
	Email	<input type="checkbox"/>
	Phone	<input type="checkbox"/>
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input type="checkbox"/>
Schedule	Student scheduled courses	<input type="checkbox"/>
	Teacher names	<input type="checkbox"/>
Special Indicator	English language learner information	<input type="checkbox"/>
	Low income status	<input type="checkbox"/>
	Medical alerts/ health data	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Student disability information	<input type="checkbox"/>
	Specialized education services (IEP or 504)	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>
	Other indicator information-Please specify:	<input type="checkbox"/>
Student Contact Information	Address	<input type="checkbox"/>
	Email	<input checked="" type="checkbox"/>
	Phone	<input type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input type="checkbox"/>
	State ID number	<input type="checkbox"/>
	Provider/App assigned student ID number	<input type="checkbox"/>
	Student app username	<input type="checkbox"/>
	Student app passwords	<input type="checkbox"/>
Student Name	First and/or Last	<input checked="" type="checkbox"/>
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	<input type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input type="checkbox"/>
Student work	Student generated content; writing, pictures, etc.	<input type="checkbox"/>

Category of Data	Elements	Check If Used by Your System
	Other student work data -Please specify:	<input type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>
	Student course grades/ performance scores	<input type="checkbox"/>
	Other transcript data - Please specify:	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>
	Other data – Please specify:	<input type="checkbox"/>
Other	<p>Please list each additional data element used, stored, or collected by your application:</p> <ul style="list-style-type: none"> • Business contact information from other client personnel such as purchasing, billing/accounting and administrators • Optional additional information about learners provided by Client admins; there are fixed fields and user-defined fields • Information attained during the execution of computer based training, answers to assessments and quizzes, and scores related to training materials. 	<input type="checkbox"/>

	<ul style="list-style-type: none"> System access/usage/interaction/authorization data 	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	<input type="checkbox"/>

EXHIBIT “C”

DEFINITIONS

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

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

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

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

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

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

Student Generated Content: The term “Student-Generated Content” means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a Contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Education Records.

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

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of Provider's services.

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

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

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such

student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

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

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

The School Board of Citrus County, Florida, Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

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

[Insert categories of data here]

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

2. Nature of Disposition

Disposition shall be by destruction or deletion of data.

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

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

As soon as commercially practicable.

____ By **[Insert Date]**

4. Signature



Authorized Representative of LEA

10/10/23
Date

5. Verification of Disposition of Data



Authorized Representative of Provider

9/14/2023
Date

EXHIBIT "E"

GENERAL OFFER OF TERMS

1. OFFER OF TERMS

Provider offers the same privacy protections found in this DPA between it and **The School Board of Citrus County, Florida** ("Originating LEA"), which is dated _____, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:

*Provider Name

BY: _____

Date: _____

Printed Name: _____

Title/Position: _____

1. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between **The School Board of Citrus County, Florida**, and the Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. ****

The School Board of Citrus County, Florida

BY: _____

Date: _____

Printed Name: _____

Title/Position: _____

SCHOOL DISTRICT NAME: THE SCHOOL BOARD OF CITRUS COUNTY, FLORIDA

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____

Title: _____

Address: _____

Telephone
Number: _____

Email: _____

EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity

Frameworks 2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider.

Cybersecurity Frameworks

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

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

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

EXHIBIT "G"

Supplemental SDPC State Terms for [State]

Version _____

[The State Supplement is an **optional** set of terms that will be generated on an as-needed basis in collaboration between the national SDPC legal working group and the State Consortia. The scope of these State Supplements will be to address any state specific data privacy statutes and their requirements to the extent that they require terms in addition to or different from the National Standard Clauses. The State Supplements will be written in a manner such that they will not be edited/updated by individual Parties and will be posted on the SDPC website to provide the authoritative version of the terms. Any changes by LEAs or Providers will be made in amendment form in an Exhibit (**Exhibit "H"** in this proposed structure).]

EXHIBIT "H"

Additional Terms or Modifications

THIS EXHIBIT "H" effective simultaneously with attached Student Data Privacy Agreement ("DPA") between The School Board of Citrus County, Florida, (the "Local Education Agency" or "LEA") and The Escal Institute of Advanced Technologies, Inc. /dba SANS Insitute, (the "Provider") is incorporated in the attached DPA and amends the DPA (and all supplemental terms and conditions and policies applicable to the DPA) as follows:

1. The second WHEREAS CLAUSE is amended to add "the Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98)" after "15 U.S.C. § 6501-6506 (16 CFR Part 312)".
2. Paragraph 3 on the page 2 of the DPA is deleted in its entirety and replaced with the following: In the event of a conflict between the DPA Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including Provider Terms of Service or Privacy Policy, the terms of Technology Master Service Agreement, and then this DPA shall control.
3. The last sentence of Article II, Paragraph 1 is amended as follows: Provider agrees that for purposes of this Agreement, it will be designated a "School Official," under the control and direction of the LEA as it pertains to the use of Student Data, with "legitimate educational interests" as those terms have been interpreted and defined under FERPA. Provider may transfer student-generated content to a separate account, according to the procedures set forth below. Provider agrees to abide by FERPA and Fla. Stat. 1002.22 while performing its service for the LEA.
4. Article I, Paragraph 2 is amended to add the following: Indemnification. Provider shall indemnify, hold harmless, and defend the SB and all of SB's current, past, and future officers, agents, and employees (collectively, "Indemnified Party") from and against any and all causes of action, demands, claims, losses, liabilities, and expenditures of any kind, including attorneys' fees, court costs, and expenses, including through the conclusion of any appellate proceedings, raised or asserted by any person or entity not a party to this Agreement, and caused or alleged to be caused, in whole or in part, by any breach of this Agreement by Provider, third-Parties, or subprocessor(s) related to Attachment A, Exhibit B (Schedule of Data), including but not limited to, failure to notify the SB of any additional students' PII collected and not updated by Provider in Exhibit B.



5. Article II, Paragraph 5 is deleted in its entirety and replaced with the following: Provider shall enter into written Agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner consistent with the terms of this DPA. Provider agrees to share the Subprocessors names and Agreements with LEA upon LEA's request.
6. Article III, Paragraph 1 is amended to add the following sentence: LEA will allow Provider access to Student Data necessary to perform the Services and pursuant to the terms of this DPA and in compliance with FERPA, COPPA, PPRA, and all other privacy statutes cited in this DPA.
7. Article IV, Paragraph 1 is amended to add the following sentence: The Parties expect and anticipate that Provider may receive personally identifiable information in education records from the District only as an incident of service or training that Provider provides to the LEA pursuant to this Agreement. The Provider shall comply with all applicable State and Federal laws and regulations pertaining to Student Data privacy and security, including FERPA, COPPA, PPRA, Florida Statutes Sections 1001.41 and 1002.22, and all other privacy statutes cited in this DPA. The Parties agree that Provider is a "school official" under FERPA and has a legitimate educational interest in personally identifiable information from education records because for purposes of the contract, Provider: (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from education records
8. Article IV, Paragraph 2 is amended to add the following sentence: Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta Student Data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.
9. Article IV, Paragraph 7 is deleted in its entirety and replaced with the following: Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, targeted advertising, or other commercial efforts by Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing

the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from generating legitimate personalized learning recommendations.

10. Article V, Paragraph 1 is deleted in its entirety and replaced with the following: Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored. Provider shall not, without the express prior written consent of District: Transmit Student Data or PII to any Providers or Subprocessors located outside of the United States; distribute, repurpose or share Student Data or PII with any Partner Systems not used for providing services to the LEA; use PII or any portion thereof to inform, influence or guide marketing or advertising efforts, or to develop a profile of a student or group of students for any commercial purpose [or for any other purposes]; use PII or any portion thereof to develop commercial products or services; use any PII for any other purpose other than in connection with the services provided to the LEA; and engage in targeted advertising, based on the Student Data collected from the LEA.
11. Article VII, is hereby amended to add Paragraph 10 as follows: **Assignment.** None of the Parties to this DPA may assign their rights, duties, or obligations under this DPA, either in whole or in part, without the prior written consent of the other party to this DPA.
12. Article VII, is hereby amended to add Paragraph 11 as follows: **Click through.** Any “click through” terms and conditions or terms of use are superseded by the Technology Master Service Agreement and this DPA, and acceptance of the terms and conditions or terms of use through the “click through” do not indicate acceptance by the entity.
13. Article VII, is hereby amended to add Paragraph 12 as follows: **Security Controls.** Security Controls. Provider represents and warrants that any software licensed hereunder shall not contain any virus, worm, Trojan Horse, tracking software or be capable of identifying non-approved users or tracking any approved user, or any undocumented software locks or drop dead devices that would render inaccessible or impair in any way the operation of the software or any other hardware, software or data for which the software is designed to work with.
14. Article VII, is hereby amended to add Paragraph 13 as follows: **Authority to Execute Agreement.** Each person signing this Agreement on behalf of either Party individually warrants that he or she has full legal power to execute this Agreement on behalf of

the Party for whom he or she is signing, and to bind and obligate such Party with respect to all provisions contained in this Agreement.

THE PARTIES REPRESENT THAT THEY HAVE THOROUGHLY DISCUSSED ALL ASPECTS OF THE AGREEMENT AND ADDENDUM WITH THEIR RESPECTIVE ATTORNEY(S), THAT THEY FULLY UNDERSTAND ALL OF ITS PROVISIONS, AND THAT THEY ARE VOLUNTARILY ENTERING INTO THE AGREEMENT AND ADDENDUM WITH THE FULL KNOWLEDGE OF ITS LEGAL SIGNIFICANCE AND WITH THE INTENT TO BE LEGALLY BOUND BY ITS TERMS.

<p>The School Board of Citrus County, Florida  _____ Douglas A. Dodd, Chairman Date: <u>10/10/23</u></p>	<p>Provider:  _____ By: Title: <u>Contracts Specialist</u> Date: <u>9/14/2023</u></p>
---	---

SANS SECURITY AWARENESS

11200 Rockville Pike, Suite 200 , North Bethesda, MD 20852, USA

ATTACHMENT B

SANS Institute - Security Awareness Price Quote

Prepared By	Keeton Ellis	Price Quote #	00059471
		Created	August 22nd, 2023
Email	kellis@sans.org	Price Quote	October 31st, 2023
Description	<p>One year of security awareness training and phishing simulation for up to 2,500 users. Training to be hosted on SANS' learning platform</p> <p>Pricing reflects best-available rates for 2023 and includes the CIS Government discounts for K12's.</p>		

Customer Contact Information

Contact Name	Lance Fletcher	Phone	3527463437 x5929
Customer Name	Citrus County Schools, FL	Email	fletcherla@citrussschools.org

Quote Line Items

Product	Quantity	Number of users	Total Price *
Enduser Security Awareness Training Licenses	2,500.00	2,500	USD 7,125.00
Engagement Materials Pack (1-5000 Users)	1.00	2,500	USD 0.00
Phishing Licenses (Bundled)	2,500.00	2,500	USD 6,750.00
	Grand Total		USD 13,875.00

Product Information

Product Description

EndUser (Stand-Alone): Customizable mix of end user training content to address relevant threats, teaching security concepts that are critical to your workplace, while adhering to the ideologies of your organization's corporate culture.

Engagement Materials Pack (1-5000): Supplemental support tools intended to reinforce and amplify the key messages taught throughout EndUser video modules.

Phishing (Bundled): Phishing awareness simulation training that reinforces the importance of security and change behavior.

Ordering and Payment Schedule

This is a Price Quote and not an Invoice. To place an order, please note the following.

- By issuing a purchase order, providing payment in response to this Price Quote, or signing this Price Quote, you are agreeing to and accepting the [SANS' Security Awareness License Agreement](#). (the "Agreement").
- If Customer has an applicable, existing, legally binding agreement with SANS ("Previous Agreement") and if there is a conflict or inconsistency between the provisions of this Agreement and any of the provisions of the Previous Agreement, the provisions of the Previous Agreement shall prevail.



SECURITY AWARENESS

11200 Rockville Pike, Suite 200 , North Bethesda, MD 20852, USA

- Although not required by SANS, Customer may issue a Purchase Order to The Escal Institute of Advanced Technologies, Inc., /dba SANS Institute for the products and services outlined in this Price Quote. It is understood and agreed that the Customer's PO is for facilitating invoicing and payment only. SANS expressly rejects any additional terms and conditions, including those which appear on a PO.
- The License Term shall begin upon the Customer's receipt of SANS' Invoice. SANS must receive payment in full within 30 days of Customer's receipt of the invoice. Acceptable payment forms include ACH, wire transfer, credit card, and check, SANS voucher account funding.
- Customer will be invoiced for one hundred percent (100%) of the Grand Total identified on this Price Quote.
- All pricing is in US Dollars.

Customer Contact Information

Client Designated Contact # 1

Client Designated Contact # 2

Name:

Name:

Title:

Title:

Email:

Email:

Phone:

Phone:


Approval

The signature below indicates agreement to the terms herein

Company: Citrus County School Board

Name: Douglas A. Dodd

Title: School Board Chairman

Signature: 

Date: 10/16/23

ATTACHMENT C

TERMS OF SERVICE

By providing payment for the Products and Services as outlined in Attachment B, CCSB ("Customer") represents it has read, understands and agrees to the following terms and conditions of this Master Services and License Agreement ("MLSA")

The following Addendums are attached and incorporated into this MLSA.

Addendum A - SSA Training Services Supplemental Terms

Addendum B – Intentionally Omitted

Addendum C - SSA Phishing Services Supplemental Terms

1. DEFINITIONS

1.1. **Affiliates** means any entity, individual, firm, or corporation, directly or indirectly, through one or more intermediaries, controlling, controlled by, or under common control with Customer.

1.2. **Applicable Data Protection Legislation** means any data protection regulation that may apply in the context of the MLSA, including, where applicable, (i) the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR") and the laws and regulations adopted to implement the GDPR and (ii) any other laws or regulations relating to the Processing of Personal Data.

1.3. **Confidential Information** means any information that is proprietary or confidential to a Party and either marked as confidential or identified as such to the other Party, including, but not limited to, business or technical data or know-how, customer and prospective customer lists, secrets, ideas, concepts, designs, drawings, flow charts, diagrams, financials, and other intellectual property, in whatever form including, documented information, machine readable or interpreted information transmitted in any form including, in writing, orally, or

visually. Any abstracts, summaries or compilations are included in this definition of Confidential Information. For avoidance of doubt, Confidential Information includes details of SANS training courses or exams, pricing, courseware, user information, and the business relationship between the Parties.

1.4. **Customer Materials** means Customer-sourced data or materials not provided by SANS or its suppliers, that are used in connection with SSA Training Materials, such as Customer-sourced content, logos, artwork, or media.

1.5. **Disclosing Party** means the Party that discloses its Confidential Information to the Receiving Party under this MLSA.

1.6. **Engagement Materials** means SANS fact sheets, FAQs, help files, media files, newsletters, posters, and screensavers provided or made available by SANS to facilitate use of the SANS Products and Services. Engagement Materials do not include SSA Training Materials themselves.

1.7. **Named User** means, as applicable, an authorized SSA Training Named User as defined in Addendum A, an authorized SSA Litmos Training Named User as defined in Addendum B, an authorized SSA Phishing Named User, as defined in Addendum C, or a named user otherwise defined in a Price Quote or additional Addendum with respect to other Services.

1.8. **Personal Data** means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

1.9. **Price Quote** means the document that details the product(s) and Services being provided to Customer by SANS, as well as the quantities, fees, Subscription Term, and payment terms.

1.10. **Processing** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means,

such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.11. **Products** means the products to be provided by SANS to Customer as set forth in a Price Quote or Statement of Work.

1.12. **Professional Services** means setup, implementation, installation, configuration or other professional Services to be provided by SANS to Customer under a Price Quote or Statement of Work.

1.13. **Receiving Party** means the Party that receives Confidential Information of the Disclosing Party under this MLSA.

1.14. **SSA Training Materials** means SANS Security Awareness videos, interactive programs, online training content, exams, assessments, electronic materials, and other training Products. Each Product is licensed separately.

1.15. **Services** means the services to be performed by SANS for Customer as set forth in a Price Quote or Statement of Work.

1.16. **Statement of Work** or **SOW** means a mutually agreed statement of Services to be performed by SANS for Customer under a Price Quote.

1.17. **Subscription Term** means the License Term or Subscription Term specified in a Price Quote.

2. SANS PROFESSIONAL SERVICES

All Professional Services will be performed in accordance with mutually agreed SOWs. Except as provided in a Price Quote or SOW for Professional Services, Customer is fully responsible for deployment of the Products and Services. SANS will only support such deployment remotely.

3. ENGAGEMENT MATERIALS

Except as set forth in the applicable Price Quote:

3.1. Customer is granted a non-exclusive, non-transferable, and non-sublicensable license during the applicable Subscription Term to use Engagement Materials related to the Products or Services to which it subscribes, only for its own internal use in connection with such Products or Services. Engagement Materials: (i) are not subject to “per user” limitations; (ii) are provided as digital files only, and (iii) may be modified or updated by SANS from time to time.

3.2. Customer shall not, for the purposes of sale, resale, lease, and/or developing a competing product: copy, reproduce, distribute, display, modify or create derivative works based upon all or any portion of the Engagement Materials in any medium.

4. TERM AND TERMINATION

4.1. The Term of this MLSA begins on the Effective Date and continues for 12 months thereafter or as identified on the applicable Price Quote; If Customer is not then in default under this MLSA, the Term shall auto-renew and extend for successive 12-month terms thereafter unless either Party provides notice of non-renewal at least sixty (60) days before the expiration of the then-current Term. The natural expiration of the Term of this MLSA shall not terminate Subscription Terms then in force, and this MLSA shall continue to govern the applicable subscriptions and Statements of Work until their respective expirations or terminations.

4.2. Subscription Term. Each Subscription Term shall be as specified in the applicable Price Quote, and if not specified, shall be twelve (12) months from the applicable Start Date. If Customer is not in default under this MLSA, and pays the applicable subscription fees for the renewal term, the Subscription Term shall auto-renew for successive 12-month terms thereafter, unless either Party provides notice of non-renewal at least sixty (60) days prior to the end of the then current Subscription Term.

4.3. Termination. Either Party may terminate this MLSA and any or all Price Quotes or Statements of Work and Subscription Terms as follows:

4.3.1. Upon thirty (30) days' written notice in the event that the other Party materially breaches, for the first time, any provision of this MLSA (a "**Default**" by the "**Defaulting Party**"), provided that the Defaulting Party's breach, if curable, has not been cured within the thirty (30) day notice period;

4.3.2. Upon thirty (30) days' written notice in the event that the Defaulting Party engages in multiple or persistent breaches of this MLSA (including but not limited to repeated non-payment) (an "**Incurable Default**"). In the event of an Incurable Default, the MLSA shall terminate regardless of any attempts by the Defaulting Party to cure.

4.3.3. Immediately if (A) the other Party ceases to carry on its business; (B) a receiver or similar officer is appointed for the other Party and is not discharged within thirty (30) days; (C) the other Party becomes insolvent, admits in writing its inability to pay debts as they mature, is adjudicated bankrupt, or makes an assignment for the benefit of its creditors or another arrangement of similar import; (D) proceedings under bankruptcy or insolvency laws are commenced by or against the other Party and are not dismissed within thirty (30) days; or (E) a Party is in default of Sections 16 or 17.

4.3.4. In the event of termination, the provisions that are intended by their terms to survive the MLSA shall survive the MLSA, which include but are not limited to: Non-Disclosure; Intellectual Property/Confidential Information; Limitation on SANS' Liability, Default, and Governing Law.

4.3.5. In the event of termination, Customer shall pay SANS for all services performed by SANS up to the date of termination, as well as all fees accrued prior to the date of termination.

4.3.6. In the event of termination of this MLSA for Default, all subscriptions, Statements of Work, and Subscription Terms hereunder shall also terminate, and Customer and its Named Users shall immediately cease all use of the licensed Products and Services.

4.4. SANS may immediately suspend Customer's and/or a Named User's access to the SLP and Services in connection with any:

4.4.1. material violation by Customer or a Named User of the use limitations or restrictions in the applicable Price Quote or Addendum or SANS' intellectual property rights;

4.4.2. technical or security issues or problems caused by Customer that materially impact the business operations of SANS or other SANS clients; and/or

4.4.3. judicial, administrative, or law enforcement orders.

4.5. Upon expiration or termination of a Subscription Term, to the extent reasonably practicable, Customer shall return (or at SANS' option destroy, and certify destruction of) all SSA Training Materials in its possession.

5. INVOICES AND PAYMENT TERMS.

5.1. Except as otherwise set forth in the Price Quote, Customer will be invoiced for one hundred percent (100%) of the total fee identified in the Price Quote.

5.2. Customer shall provide payment within 30 days of invoice receipt.

5.3. Taxes. Customer and/or its Affiliates shall be liable for all sales, use, value added, duties, tariffs or other similar taxes of any nature whatsoever associated with the provision of Training or other products or services provided under this MLSA. Customer shall provide SANS with a copy of all applicable tax exemption certificates.

5.4. Payment Forms. Acceptable payment forms include ACH, wire transfer, credit card, check, and SANS voucher account funding. Customer is responsible for any applicable fees associated with the payment form.

6. AUDIT

During the Term, SANS will keep true and accurate books and records relating to this procurement (collectively, "Records"). Records will include such information

necessary for the Customer to verify the accuracy of the invoicing, billing, and payments in connection with the ordered services delivered hereunder, but not the underlying costs and financial data used in calculating the same. At the Customer's reasonable request, SANS will provide access to the Records, as necessary, to verify the fees and other amounts charged to the Customer, which shall be accomplished through electronic means.

7. INTELLECTUAL PROPERTY/CONFIDENTIAL INFORMATION

7.1. Customer acknowledges that SANS or its licensors are the sole and exclusive owners of the SANS Products and Services, and the SANS Confidential Information, including, without limitation, the SSA Training Materials and the Engagement Materials, and any improvements and enhancements thereto and derivations thereof, and all intellectual property rights therein. Nothing in this MLSA transfers SANS' exclusive ownership of its intellectual property or Confidential Information.

7.2. Customer may not: (i) except as expressly provided in this MLSA, use, copy, modify, translate, or merge any such information or create derivative works therefrom; (ii) disable or circumvent any SANS licensing control feature; (iii) reverse-engineer, disassemble, or decompile such information, or otherwise attempt to access or determine its underlying source code, underlying user interface techniques or algorithms, or permit any such actions; (iv) distribute, lend, sublicense, rent or lease the above; and/or (v) attempt to build a competitive service or product, or copy any feature, function or graphic for competitive purposes.

7.3. SANS acknowledges that Customer or its licensors are the sole and exclusive owners of the Customer Materials and Customer Confidential Information, and all intellectual property rights therein. Nothing in this MLSA transfers Customer's exclusive ownership of its intellectual property or Confidential Information.

8. CONFIDENTIALITY

8.1. A Receiving Party may be given Confidential Information from the Disclosing Party in order to perform its obligations under this MLSA. The Receiving Party

will protect the confidentiality of the Disclosing Party's Confidential Information during the Term of this MLSA and indefinitely thereafter by (a) using the same means it uses to protect its own Confidential Information, but in any event, not less than reasonable means, and (b) using the Disclosing Party's Confidential Information solely in connection with this MLSA. The Receiving Party shall not copy or disclose this MLSA and the Disclosing Party's Confidential Information except to those employees, officers, directors, subcontractors, agents, or affiliates of the Receiving Party ("Representatives") who have a need to know such Confidential Information as required in connection with this MLSA; provided, such Representatives are advised of and agree to abide by the confidentiality obligations set forth in this MLSA. Compliance by Representatives with the confidentiality and use obligations in this MLSA will remain the responsibility of Receiving Party, and both Receiving Party and Representatives shall be liable for any breach of this MLSA by Representatives.

8.2. The Receiving Party may be given Confidential Information from the Disclosing Party in order to perform its obligations under this MLSA. The Receiving Party will protect the confidentiality of the Disclosing Party's Confidential Information during the Term of this MLSA and indefinitely thereafter by (a) using the same means it uses to protect its own Confidential Information, but in any event, not less than reasonable means, and (b) using the Disclosing Party's Confidential Information solely in connection with this MLSA. The Receiving Party shall not copy or disclose this MLSA and the Disclosing Party's Confidential Information except to those employees, officers, directors, subcontractors, agents, or affiliated entities of the Receiving Party ("Representatives") who have a need to know such Confidential Information as required in connection with this MLSA; provided, such Representatives are advised of and agree to abide by the confidentiality obligations set forth in this MLSA. Compliance by Representatives with the confidentiality and use obligations in this MLSA will remain the responsibility of Receiving Party, and both Receiving Party and Representatives shall be liable for any breach of this MLSA by Representatives.

8.3. Confidential Information will not include any information or data which:

8.3.1. was rightfully in the Receiving Party or its Representatives' possession prior to receipt from the Disclosing Party;

8.3.2. becomes rightfully available to the Receiving Party or its Representatives from a source other than the Disclosing Party who is free to lawfully disclose such information to the Receiving Party;

8.3.3. is independently developed by the Receiving Party or its Representatives, without the use of the Disclosing Party's Confidential Information; or

8.3.4. is legally required to be disclosed to a regulatory agency or pursuant to an order of a court of competent jurisdiction, provided that, where permissible, the Disclosing Party be given an opportunity to seek a protective order.

8.4. ***Applicable only if Customer is a governmental entity:*** In the event SANS, as the Disclosing Party, identifies its information as Confidential Information, and Receiving Party is a government entity and can demonstrate that SANS' Confidential Information would otherwise be public information based upon governing law, then prior to public disclosure, the Receiving Party, as a government entity, shall provide SANS written notice demonstrating SANS' Confidential Information would otherwise be public information based upon governing law.

8.5. Upon termination of this MLSA, at Disclosing Party's request and to the extent legally permissible (as interpreted by SANS), Receiving Party will destroy or return to Disclosing Party all Disclosing Party's Confidential Information in its possession or control and provide written certification of compliance thereof.

8.6. Receiving Party agrees to take appropriate actions to address incidents of unauthorized access to Disclosing Party's Confidential Information, including notification within five (5) days to Disclosing Party of any such incident.

9. DATA PROTECTION

9.1. In order to perform the Services under this MLSA, SANS is required to Process Personal Data. SANS shall comply with the Applicable Data Protection Legislation.

9.2. With respect to Personal Data, the Customer shall act as a Personal Data Controller, where “Controller” means the entity which alone determines the purposes and the means of the Processing of Personal Data, and SANS shall carry out the Processing of the Personal Data only on behalf of the Customer. Acting as a Data Processor, SANS shall carry out the Processing of Personal Data only according to the Customer’s documented instructions for Processing, unless that law prohibits such information on important grounds of public interest.

9.3. To the extent that data includes Personal Data, the Parties agree that the SANS DPA is incorporated into these terms and applies automatically to all customers globally who require it.

9.4. To the extent that Personal Data is provided from a Party to the other Party and such disclosure requires a data processing agreement between the Parties under an applicable data protection law , the Parties agree that the SANS DPA is incorporated into and attached to this MLSA by reference.

10. REPRESENTATIONS AND WARRANTIES

10.1. Each Party represents and warrants to the other Party:

10.1.1. it is duly organized and in good standing in the state or jurisdiction in which is it incorporated or organized;

10.1.2. it has full right and power to enter into this MLSA, and the signer of this MLSA has authority to bind such Party it signs on its behalf;

10.1.3. it is not prohibited by any regulatory authority from carrying out its duties and obligations under this MLSA.

10.2. Such representations and warranties shall be continuing throughout the Term of this MLSA.

10.3. SANS represents and warrants to Customer:

11. INTELLECTUAL PROPERTY INDEMNIFICATION

11.1. Subject to the limitations of liability in Section 14, SANS shall defend, indemnify, and hold Customer and its officers, directors, employees, and agents (each a “**Customer Indemnitee**”) harmless from and against any third party claims, demands, suits, proceedings, and resulting liabilities, direct damages, and expenses (collectively “**Claims**”), to the extent that the SSA Training Services, SSA Training Materials, SSA Phishing Services, or Engagement Materials infringe any patent, copyright, trademark, trade secret or other intellectual property interest of a third party. SANS shall, in its sole discretion and at no additional charge to Customer, make commercially reasonable efforts to replace, in whole or in part, the infringing materials or Services with substantially compatible and functionally equivalent materials or Services, modify them to avoid the infringement, or secure the right for Customer to continue their use. In the event that SANS determines that the foregoing actions are not commercially practicable, either Party may terminate the applicable Price Quote, and SANS shall refund to the Customer the applicable subscription fees for periods after the effective date of termination. This obligation does not extend to infringement by any Customer Materials incorporated into the foregoing, or to infringement resulting from any modifications or adaptations made by Customer or third parties to the foregoing.

11.2. Subject to the limitations of liability in Section 14, Customer shall defend, indemnify, and hold SANS and its officers, directors, employees, and agents (each a “**SANS Indemnitee**”) harmless from and against any Claims alleging that the Customer Materials infringe any patent, copyright, trademark, trade secret or other intellectual property interest of a third party.

11.3. The foregoing obligations are conditioned on (i) the Customer Indemnitee or SANS Indemnitee (each an “Indemnitee” as applicable) providing prompt notification of the Claim to the other indemnifying Party (SANS and Customer each the “Indemnifying Party” as applicable), (ii) the Indemnitee allowing the Indemnifying Party to control the defense and settlement of the Claim (except that the Indemnifying Party may not agree to any settlement or consent to any judgment that would admit fault, wrongdoing or liability on the part of the Indemnitee without such Indemnitee’s prior written consent), and (iii) the Indemnitee’s cooperation with the Indemnifying Party as reasonably requested

by the Indemnifying Party (at the Indemnifying Party's expense) in the defense and any related settlement of the Claim.

11.4. **Applicable only if Customer is a governmental entity:** To the extent established law preempts or limits Customer from providing indemnification to SANS, each Party's indemnification obligation in this section shall be eliminated or mutually limited pursuant to applicable law to Customer.

12. GENERAL INDEMNIFICATION

12.1. Subject to the limitations of liability in Section 11, each Indemnifying Party agrees to indemnify, defend and hold harmless the other Party's Indemnitee against any and all losses, damages, liabilities or expenses (including reasonable attorneys' fees and other costs of defense) in connection with any and all actions, suits, claims or demands that may be brought or instituted against any Indemnitee by any third party to the extent they arise out of or relate to (a) a breach of a representation, warranty or covenant of the Indemnifying Party under this MLSA, or (b) an Indemnifying Party's negligence or willful misconduct in performing obligations under this MLSA.

12.2. The foregoing obligations are conditioned on (i) the Indemnitee's prompt notification of the Claim to the Indemnifying Party, (ii) the Indemnitee allowing the Indemnifying Party to control the defense and settlement of the Claim (except that the Indemnifying Party may not agree to any settlement or consent to any judgment that would admit fault, wrongdoing or liability on the part of the Indemnitee without such Indemnitee's prior written consent), and (iii) the Indemnitee's cooperation with the Indemnifying Party as reasonably requested by the Indemnifying Party (at the Indemnifying Party's expense) in the defense and any related settlement of the Claim.

13. DISCLAIMER OF WARRANTY AND LIMITATIONS OF LIABILITY

13.1. IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, EXEMPLARY, OR PUNITIVE DAMAGES OR LIABILITIES OR FOR ANY LOST PROFITS, LOST SAVINGS OR LOSS OF REVENUES, ARISING FROM OR RELATING TO THIS MLSA OR THE SANS

PRODUCTS OR SERVICES, EVEN IF THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

13.2. IN NO EVENT SHALL SANS' LIABILITY IN ANY MANNER ARISING UNDER THIS MLSA EXCEED THE TOTAL PAYMENT RECEIVED BY SANS UNDER THE PRICE QUOTE FOR THE SANS PRODUCTS OR SERVICES FROM WHICH THE CLAIM ARISES DURING THE 12-MONTH PERIOD IMMEDIATELY PRECEDING THE DATE WHEN THE CAUSE OF ACTION ARISES.

14. INSURANCE

SANS shall, at its sole expense and throughout the Term, carry and maintain the following insurance coverage: (a) Commercial General Liability, (b) Worker's Compensation; and (c) Employer's Liability, in reasonable amounts.

15. COMPLIANCE WITH LAWS

15.1. Each Party will, at its sole expense, obtain all permits and licenses, pay all fees, and comply with all federal, state, and local laws, ordinances, rules, regulations, codes, and orders applicable to it in the performance of this MLSA.

15.2. Each Party shall conduct operations in compliance with applicable laws, rules and regulations in exercising rights and obligations under any part of this MLSA. Laws may include but not be limited to the U.S. Foreign Corrupt Practices Act, the U.K. Bribery Act and local anticorruption legislation that may apply. Neither party is listed by any government agency as debarred, suspended, proposed for suspension or debarment or otherwise determined to be ineligible for government procurement programs. In exercising rights and obligations under any part of this MLSA, neither party nor anyone acting on its behalf shall make, offer, promise or authorize payment of anything of value directly or indirectly to any of the following prohibited parties for the purpose of unlawfully influencing their acts or decisions: a) employees, consultants, or representatives of the other Party, b) government officials or employees, c) political party officials or candidates, d) officers or employees of any public international organization, e) immediate family member of such persons (or any other person) for the benefit of such persons.

15.3. Each Party warrants that neither it nor its controlling owners is listed on any (i) sanction programs list maintained by the U.S. Office of Foreign Assets Control within the U.S. Treasury Department (“OFAC”), or (ii) denied party list maintained by the U.S. Bureau of Industry and Security within the U.S. Department of Commerce (“BIS”). Customer agrees it shall not allow Users access to any SANS product, service, or technology provided under this MLSA to any person or entity in a U.S. embargoed country or in violation of a U.S. export control law or regulations. Customer agrees to cooperate with SANS as necessary for SANS to comply with export requirements and recordkeeping required by OFAC, BIS, or other governmental agency.

16. GOVERNING LAW; JURISDICTION; ATTORNEY’S FEES

This MLSA will be governed by and construed in accordance with the laws of the State of Maryland. Each party hereby irrevocably consents to exclusive personal jurisdiction and venue in the state and federal courts located in Maryland. Any This MLSA will be governed by and construed in accordance with the laws of the State of Maryland. Each party hereby irrevocably consents to exclusive personal jurisdiction and venue in the state and federal courts located in Maryland. Both Parties exclude the application of the Uniform Computer Information Transactions Act (“UCITA”), the United Nations Convention on the International Sale of Goods (“CISG”) and any law of any jurisdiction that would apply UCITA or CISG or terms equivalent to UCITA or CISG to this MLSA. The Parties agree to settle all disputes promptly by negotiation between executives in good faith. Should good faith negotiations fail, any controversy or claim arising out of or relating to this MLSA, or breach thereof, will be exclusively settled by binding arbitration in Montgomery County, Maryland, USA administered by the American Arbitration Association in accordance with its Commercial Arbitration Rules, and judgment on the award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof. Either party may initiate arbitration by written notice if negotiations have failed to resolve the matter within 30 days of initiation. The language of the arbitration will be English.

17. NOTICES

All notices or reports required or permitted under this MLSA shall be in writing and shall be delivered by personal delivery, facsimile transmission, a nationally recognized overnight delivery service, by certified or registered mail, return receipt requested, or by electronic mail to be confirmed in writing delivered by one of the methods described herein, and shall be deemed given upon personal delivery, electronic confirmation of electronic mail or facsimile transmission, or signature evidencing receipt of overnight delivery or registered mail, as applicable. Notices and communications between Customer and SANS shall be in English to the following addresses of the Parties or to such other addresses as the Party concerned may subsequently notify in writing to the other Party. Notice hereunder shall be delivered to the Parties' at the addresses listed on the applicable Price Quote with attention to the Legal Department.

18. EXPORT COMPLIANCE

The Products, Services and other technology provided under this MLSA may be subject to export laws and regulations of the United States of America and other jurisdictions. Each Party warrants that neither it nor its controlling owners is (i) listed on any sanction programs list maintained by the U.S. Office of Foreign Assets Control within the U.S. Treasury Department ("OFAC"), or (ii) denied party list maintained by the U.S. Bureau of Industry and Security within the U.S. Department of Commerce ("BIS"). Customer agrees it shall not allow users access to any Product, Service or technology provided under this MLSA to any person or entity in a U.S. embargoed country or in violation of a U.S. export control law or regulations. Customer agrees to cooperate with SANS as necessary for SANS to comply with export requirements and recordkeeping required by OFAC, BIS or other governmental agency.

19. MISCELLANEOUS

19.1. Assignment; No Third-Party Beneficiaries. Neither Party may assign this MLSA or its rights or obligations thereunder without the written consent of the other Party, which consent will not be unreasonably withheld, except that a Party may assign upon written notice to a successor by merger, acquisition, or sale of substantially all of such Party's business or assets. In addition, SANS may assign this MLSA or applicable Price Quotes in whole or part to an affiliated

entity without written consent of Customer. SANS may subcontract all or any part of its obligations under this MLSA or applicable Price Quotes but shall remain responsible for the acts and omissions of its subcontractors as though they were acts of SANS itself. Except as specifically provided herein, there are no third-party beneficiaries to this MLSA, and nothing in this MLSA shall benefit or create any right on behalf of any person or entity other than Customer and SANS.

19.2. Waiver. The failure of either Party to exercise or enforce any right or provision of this MLSA shall not constitute a waiver of such right or provision or a waiver of the right of such Party to thereafter enforce each and every provision of this MLSA.

19.3. Severability. If a particular provision of this MLSA is terminated or held by a court of competent jurisdiction to be invalid, illegal, or unenforceable, that provision of the MLSA will be enforced to the maximum extent legally permissible and the remainder of this MLSA will continue in full force and effect.

19.4. Headings. The headings or titles preceding the text of the sections and subsections of this MLSA are inserted solely for convenience of reference, and shall not constitute a part of this MLSA, nor shall they affect the meaning, construction or effect of this MLSA.

19.5. Independent Contractor. SANS is an independent contractor and not an employee, agent, affiliate, partner or joint venturer with or of Customer.

19.6. Force Majeure. Neither Party shall be liable to the extent that its performance of this MLSA is prevented, or rendered so difficult or expensive as to be commercially impracticable, by reason of an Act of God, labor dispute, unavailability of transportation, goods or services, governmental restrictions or actions, war (declared or undeclared) or other hostilities, pandemic, or by any other event, condition or cause which is not foreseeable on the Effective Date and is beyond the reasonable control of the Party, provided that such Party promptly informs the other Party of such event, and makes diligent efforts to work around the event and resume performance. In the event of non-performance or delay in performance attributable to any such causes, the period

allowed for performance of the applicable obligation under this MLSA will be extended for a period equal to the period of the delay.

19.7. Entire Agreement. This MLSA and all appendices attached hereto (which are specifically incorporated herein by this reference) contain the full and entire agreement between the Parties. It supersedes all prior negotiations, and proposals, written or otherwise, relating to its subject matter. Any modifications, revisions or amendments to this MLSA must be set forth in writing signed by authorized representatives of both Parties.

19.8. Customer PO to Facilitate Payment Only. The Parties agree that any PO submitted by a Customer to SANS is for facilitating invoicing and payment only. Any additional, inconsistent, or different terms included in a Customer PO or other documents (including electronic) submitted to SANS by or on behalf of Customer at any time, whether before or after the Effective Date are hereby expressly rejected by SANS and of no effect. These terms and conditions shall be deemed accepted by Customer without any such additional, inconsistent, or different terms and conditions, except to the extent expressly accepted by SANS in writing and signed by SANS.

19.9. Counterparts. This MLSA may be executed and delivered (i) in any number of counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument, and/or (ii) by exchange of facsimile or PDF copies, or secure electronic signature and delivery method (e.g., DocuSign), in which case the instruments so executed and delivered shall be binding and effective for all purposes.

ADDENDUM A

SSA TRAINING SERVICES SUPPLEMENTAL TERMS

1. SUPPLEMENTAL DEFINITIONS

1.1. **Customer Learning Management System or Customer LMS** means a Customer-supplied software application for the administration, documentation, tracking, reporting, and delivery of educational courses, training programs, or learning and development programs.

1.2. **SSA Learning Platform or SLP** means a training platform owned and operated by SANS to deliver online training. SANS reserves the right to upgrade its platform or migrate it to another, with this MLSA remaining in full force and applying equally to any upgraded or new platform(s).

1.3. **SSA Training Named User** means any individual who has been issued a user login account at any time during the Subscription Term permitting such individual to access and use SSA Training Materials through the SLP or the Customer LMS as applicable. An SSA Training Named User must be an employee, agent, contractor, or representative of Customer unless otherwise authorized by SANS.

1.4. **SSA Training Services** means the provision by SANS of SSA Training Materials or related services to Customer or its SSA Training Named Users.

2. SSA TRAINING SERVICES. Except as set forth in the Price Quote:

2.1. Customer is granted a non-exclusive, non-transferable, and non-sublicensable license during the Subscription Term to access and use the SLP solely to administer the delivery of SSA Training Services to SSA Training Named Users; add or delete SSA Training Named Users; assign training; run reports; customize themes; customize system notification messages; enable SSA Training Named Users to view SSA Training Materials and receive SSA Training Services, and to the extent specifically authorized by SANS; supplement SSA Training Materials with training materials related to the SSA Training Materials for

presentation to SSA Training Named Users. Use of SSA Training Services for delivery of any other content is strictly prohibited.

2.2. Customer may permit SSA Training Named Users to access and use the SSA Training Materials through the SLP during the Subscription Term to view SSA Training Materials and receive SSA Training Services.

2.3. Use of SSA Training Materials during the Subscription Term is limited to no more than the number of SSA Training Named Users set forth in the Price Quote.

2.4. Each of the SSA Training Materials will have a separate SSA Training Named User account.

2.5. Customer grants SANS all necessary rights to authorize it and its affiliates and subprocessors a non-exclusive right to process data solely to provide the SSA Training Services and Litmos functionality (as applicable) described in this MLSA to Customer and its SSA Training Named Users.

2.6. Customer shall:

2.6.1. ensure that its SSA Training Named Users comply with the terms of this MLSA and shall be responsible for the acts or omissions of any SSA Training Named User, or person using an SSA Training Named User's login, in connection with their use of the SSA Training Materials, or access to Litmos or the SLP not in conformity with this MLSA;

2.6.2. notify SANS within five (5) business days of any known unauthorized use of Customer's or any SSA Training Named User's account;

2.6.3. not copy, reproduce, distribute, display, modify or create derivative works based upon all or any portion of Litmos or the SSA Training Materials in any medium, without the express written consent of SANS, or permit any other person to do so;

2.6.4. not sell, resell, rent, or lease the SSA Training Materials or access to Litmos or the SLP, or permit any other person to do so;

2.6.5. not interfere with or disrupt the performance of Litmos or the SLP, or permit any other person to do so;

2.6.6. not provide access to anyone other than an authorized SSA Training Named User;

2.6.7. not attempt to gain unauthorized access to Litmos, the SLP, or any CBT Material, or permit any other person to do so.

3. SSA TRAINING NAMED USERS AND LEARNING PLATFORM

3.1. Each individual permitted to access or use a component of the SLP must be assigned a unique user login and will be considered an SSA Training Named User. Customer may not permit more than one person to access or share a single user login account, nor otherwise attempt to circumvent licensing metrics.

3.2. Once credentialed, an SSA Training Named User continues to be counted in the SSA Training Named User metrics even if that SSA Training Named User ceases to have a login account. New SSA Training Named Users must be added and may not be substituted for prior SSA Training Named Users.

3.3. Customer must adhere to SANS' reasonable guidelines to ensure system performance, including those regarding data purging, hosting hardware and infrastructure, and loads per instance.

3.4. SANS reserves the right to limit the number of SSA Training Named Users eligible for SANS training for system performance.

3.5. Customer may not use the SLP: (i) to deliver any training other than SSA training; (ii) to deliver training or manage data on behalf of any other organization; (iii) to provide software or content development services to third parties; (iv) on a service bureau or time-share basis; and/or (v) as an application service provider.

3.6. Customer may not, at any time, load users onto the SLP in excess of 1.05 times the number of Named Users set forth in the MLSA and/or Price Quote.

ADDENDUM B

Intentionally omitted.

ADDENDUM C

SSA PHISHING SERVICE SUPPLEMENTAL TERMS

Except as set forth in the applicable Price Quote, the following supplemental terms and conditions shall apply to Customer's use of the SSA Phishing Service:

1. Supplemental Definitions

1.1. **SSA Phishing Named User** means any individual (i) with a user login account permitting such individual to access and use SSA Training Materials on the SLP or Customer LMS, or (ii) designated to be tested in SSA Phishing Service activities.

1.2. **SSA Phishing Service** means a SANS tool or service available to Customer to test its employees' ability to withstand phishing/social engineering attacks.

2. Customer is hereby granted a non-exclusive, non-transferable, and non-sublicensable license, to use the SSA Phishing Service during the Subscription Term set forth in the Price Quote, limited to the number of SSA Phishing Named Users set forth in the Price Quote.

3. Customer grants SANS all necessary rights to authorize SANS and its subprocessors a non-exclusive right to process data solely to provide the SSA Phishing Service to Customer and its SSA Phishing Named Users.

4. A person who is a user only because he or she is designated to be tested through the SSA Phishing Service will not be counted against Customer's total allotment of SSA Phishing Named Users until the first phishing message is sent to that SSA Phishing Named User by the SSA Phishing Service, at which point the he/she will become an SSA Phishing Named User.

5. Customer shall:

5.1. ensure that its SSA Phishing Named Users comply with the terms of this MLSA and shall be responsible for the acts or omissions of any SSA Phishing

Named User, or person using an SSA Phishing Named User's login, in connection with their use of the SSA Phishing Services not in conformity with this MLSA;

5.2. notify SANS within five (5) business days of any known unauthorized use of Customer's account;

5.3. not attempt to gain unauthorized access to or reverse engineer the SSA Phishing Service;

5.4. not use any SANS Confidential Information to build a competitive service or product, nor copy any feature, function or graphic for competitive purposes;

5.5. not sell, resell, rent or lease the SSA Phishing Service; and

5.6. only conduct simulated phishing emails to domains and recipients for whom Customer has authorization.

6. If third party services or applications are provided to Customer as part of the SSA Phishing Services, Customer shall protect the confidential and proprietary information of such third parties to the same degree as it is obligated to protect other Confidential Information under the MLSA.

7. Neither Party shall utilize any phishing practices or templates that would create a significant risk of claims, liabilities, administrative actions, internet service provider blacklisting, or other consequences adverse to either SANS or Customer, such as identification of the sender as the Internal Revenue Service or another government agency or violations of industry standard acceptable use policies. SANS and its service providers may, but are not obligated to, take action to prevent and stop transmission of any such content provided by Customer.

ATTACHMENT D

PRIVACY POLICY

Updated: December 2022

SANS INSTITUTE PRIVACY POLICY

The Escal Institute of Advanced Technologies, Inc. d/b/the SANS Institute (referred throughout as “SANS”) is a US based company specializing in information security and cybersecurity training. SANS also operates its Global Information Assurance Certification (“GIAC”) programs and academic programs offered through the SANS Technical Institute (“STI”).

This Policy addresses how SANS, as a data controller, collects, uses, and otherwise processes personal information relating to individuals who visit our Websites and use our services, as well as personal information that is collected from business partners and via survey responses or competition entries.

When we refer to “Websites” we mean www.sans.org as well as the other websites that we operate and that link to this Policy. Note that GIAC has its own privacy policy at www.giac/privacy, and SANS Technical Institute has its own Privacy Policy at www.sans.edu/privacy. This Policy does not apply to personal information collected and processed by GIAC or the SANS Technical Institute.

We need to process personal information to provide services to you. Sometimes, we provide your personal information to third parties to help us provide our services. If you are not willing to provide your personal information and have it disclosed to third parties in accordance with this Privacy Policy, you may not be able to use our services.

Basis of Processing

On most occasions we process your data based on your consent or because the processing is necessary for us to fulfill our contractual obligations to you. You do not have to provide consent when we request it, however you may be unable to use some of our services if you do not allow us to process your personal data.

Our Websites may contain links to other websites which are not owned by SANS. You should review the privacy statements of all third-party websites you visit to understand how your data will be processed.

Personal Information We Collect

You will be asked to provide personal data when you create a SANS account, make a purchase, or contact us for support. We also collect data recording how you interact with our services. We may also obtain information about you from our business partners or other third parties.

We may receive and collect certain data automatically for example from website analytics, information from your internet browser when you visit our Websites, and information collected by cookies. We may collect Personal Information that can identify you, such as your name and email address, and other information that does not identify you.

Information Provided by You

When You Set Up a SANS Account

We collect your name, email address, phone number(s), address, company, department, job function, industry, organizational memberships, and geographic region to create a SANS account. We also process and store data associated with training assignments, including scores on assessments you undertake, data associated with your registration for content such as webcasts and Summits, and data associated with your use of content provided by our Websites.

When You Use Our Websites

We use various technologies to collect information from your computer or device and about your activities on our Websites. These are detailed below:

1. **Information automatically collected** such as your IP address, your browser type and language, access times, the content of any undeleted cookies that your browser previously accepted from us, referring or exit website address, internet service provider, date/time stamp, operating system, locale and language preferences, and system configuration information.
2. **Cookies.** When you visit our Websites we may assign your computer or device one or more cookies to facilitate access to our site and to personalize your online experience. These cookies may relate to tools such as Google Analytics and similar technologies. Through cookies we also may automatically collect information about your online activity on our site, such as the web pages you visit, the links you click, and the searches you conduct on our site. Please see our [Cookie Policy](#) for more detail.
3. **Other technologies.** We may use standard internet technology, such as web beacons, session replay scripts, and other similar technologies, to track your use of our Websites. We also may include web beacons in promotional email messages or newsletters. Web beacons are tiny graphics with a unique identifier, similar in function to cookies. In contrast to cookies, which are stored on your computer's hard

drive, pixel tags are embedded invisibly on web pages. We may use these, in connection with our Websites to, among other things, track the activities users of our services, improve ads, personalize and manage content, and gather usage information about our Websites. We may also use these in HTML emails to, to help us track email response rates, identify when our emails are viewed, and track whether our emails are forwarded. Session replay software scripts capture information concerning a user's interaction with the Websites, including keystrokes, mouse movements and clicks, movements within a webpage and through the Websites, interactions with menus, banners, and forms, and form field entries. We may use third-party software embedded in the script of the Websites to monitor your interaction with the Websites and/or for our compliance verification purposes, which may mean that the third-party software provider also collects this information. By using our Websites, you consent to this collection and disclosure of information.

Information Collected from Other Sources

We may also obtain information about you from advertising companies, ad networks business partners, contractors, and other third parties and add it to our account information or other information we have collected. We only do this where there is a lawful basis of processing your information such as your consent.

Information Collected for Employer-Sponsored Training

If your employer sponsors your training and provides us with your Personal Information, SANS acts as a data controller and your employer is also a data controller. SANS will work with your employer to fulfill any data rights requests. Your information and training records will be shared with your employer and we will process that information in accordance with this Privacy Policy.

How We Use Personal Information

We use the Personal Information we collect for a variety of purposes. The legal basis for our processing of Personal Information will depend on the context in which we collect it.

General Uses

We may use information that we collect about you to:

- deliver the services that you have requested
- manage your account and provide you with customer support

- perform research and analysis about your use of or interest in our services, our content, or products, as well as services or content offered by others
- communicate with you by email, postal mail, telephone, our websites, our applications, and/or mobile devices about products, services, or resources that may be of interest to you either from us or other third parties
- enforce our terms and conditions
- manage our business and perform functions as otherwise described to you at the time of collection
- for legal compliance purposes
- occasionally notify you about special sales or services to personalize your experience with SANS (you can opt out if you wish)
- process payment for any purchases or sales made on our Websites, to protect against or identify possible fraudulent transactions, and otherwise as needed to manage our business

How Long We Retain Your Personal Information

We will retain your Personal Information for as long as is needed to offer you services or comply with our legal obligations. For Personal Information that we process on behalf of a business partner or your employer, we will retain such Personal Information in accordance with the terms of our agreement with them.

Disclosure of Personal Information

We share or disclose your Personal Information where it is necessary to provide the Services, including sharing information with third party service providers, when required by law, to protect rights and safety, and with your consent. These third parties are detailed below.

- **Authorized service providers:** These services may include fulfilling orders, processing credit card payments, delivering materials, providing customer service and marketing assistance, performing business and sales analysis, supporting our Websites' functionality, and supporting contests, promotions, sweepstakes, surveys and other features offered through our Websites. These service providers may have access to Personal Information needed to perform their functions but are not permitted to share or use such information for any other purposes.
- **Co-Sponsoring organizations:** Some SANS training events are co-sponsored by other organizations. Examples include SANS private training events, sponsored webcasts, or sponsored whitepapers. When you register for an event, the co-sponsoring organization may have access to your registration data where you agree and provide your explicit consent.

- **GIAC Certification Information:** GIAC Certified Professionals are listed on the GIAC website and their identities and certifications are considered public information. Published data includes Analyst Number, Certification Holder's Name and Certification Expiration Date. No personal contact information is published.
- **Business partners:** When you make purchases or engage in promotions offered through our Websites, we may share Personal Information with your consent with the businesses with which we partner to offer you those services, promotions, contests and/or sweepstakes.
- **Business transfers:** We may disclose and/or transfer personal information as part of any actual or contemplated merger, sale, transfer of assets, acquisition, financing and/or restructuring of all or part of our business, bankruptcy or similar event, including related to due diligence conducted prior to such event when permitted by law.
- **Protect our rights:** We may disclose personal information where we believe it necessary to respond to claims asserted against us, to comply with legal process (e.g., subpoenas or warrants), enforce or administer our agreements and terms, for fraud prevention, risk assessment, investigation and/or to protect the rights, property or safety of our company, our customers and/or others.
- **Other situations:** We also may disclose your information where required by law, in response to a court order, or to prevent or detect crime.
- **Aggregated and Non-personal Information:** We may share aggregated and non-personal information we collect under any of the circumstances set forth in this Policy. When we de-identify personal information, we have implemented reasonable measures as required by law to ensure that the de-identified data cannot be associated with any individual or customer. We will only maintain and use such data in a de-identified manner and do not attempt to re-identify the data, except as permitted by law.

In general, we may disclose the following categories of personal information in support of our business purposes identified above:

- Name, contact information, and other identifiers
- Customer records
- Protected classifications
- Commercial Information
- Usage data
- Audio, video, and other electronic data
- Education information
- Profiles and inferences

We have disclosed the categories of personal information listed above to the following categories of third parties in the preceding twelve months: data analytics providers, service providers, and sponsors of SANS events, programs, and papers.

Categories of Personal Information Sold or Shared.

The California Consumer Privacy Act (“CCPA”) defines a “sale” as disclosing or making available to a third party personal information in exchange for monetary or other valuable consideration, and it defines “share” in pertinent part as disclosing personal information to a third party for cross-context behavioral advertising.

As defined by the CCPA, the categories of personal information that we may “sell” include:

- Name, contact information and other identifiers

As defined by the CCPA, the categories of personal information that we may “share” include:

- Name, contact information, and other identifiers

The categories of third parties to whom we sell or share the data, as defined by the CCPA, may include:

- Data analytics providers
- Service providers who are assisting us in fulfilling our contracts and carrying out our business
- Sponsors of SANS events, programs and papers

The business purpose for which we sell or share the data, as defined by the CCPA, may include:

- Lead generation, business prospecting, and similar activities
- To gain insights into online activities through analytics
- To provide leads to sponsors of SANS events, programs and papers

We have “sold” and “shared” the categories of personal information listed above to data analytics providers in the preceding twelve months.

Your Privacy Rights

How You Can Access Your Information

If you have an online account with us, you can review your Personal Information by logging into your account. You can also update your Personal Information by contacting us.

You can ask us to delete, rectify, or port your data by submitting a request through your account or by contacting privacy@sans.org.

We will handle your request as soon as possible; however, we may still need to retain certain information, for example information required for legal purposes.

Opt-Out

We will not share personal data without your permission unless it is necessary for us to provide services to you.

You can opt out of non-essential use of your data at any time by selecting the “Opt-Out” link found in the footer of the communication or on our Websites and following the instructions or contacting us.

If you opt out of receiving promotional communications, you may continue to receive emails and notifications relating to business-related communications.

Additional Information for Residents of Certain Jurisdictions

For Residents of the European Union and the United Kingdom

If you are a resident of the European Union or United Kingdom, the E.U. or U.K. General Data Protection Regulation (collectively, the “GDPR”) is applicable to our use of your data. The lawful basis for processing your personal information will depend on the personal information concerned and the specific context in which we collect it as detailed above. Under the GDPR you have a number of rights. For example, you can request to see a copy of the data we process about you, to delete or rectify your data, or to transfer your data elsewhere. You also have the right to make a complaint to your local supervisory authority and in the first instance to our Data Privacy Department.

If you wish to exert any of your rights, please contact us at via email at privacy@sans.org.

You should be aware that your Personal Information may be transferred to, stored, and processed within the United States and other jurisdictions outside of the U.S.A., the E.U. or the U.K. We will take all appropriate measures to safeguard your information including applying standard contractual clauses.

For Residents of California

- **Right to Know:** You have the right to request that a business that collects personal information about you disclose the following: (1) the categories of personal information it has collected about you; (2) the categories of sources from which the personal information is collected; (3) the business or commercial purpose for collecting, selling, or sharing personal information; (4) the categories of third parties to whom the business discloses personal information; and (5) the specific pieces of personal information it has collected about you.
- **Right to Correct:** You have the right to request a business that maintains inaccurate personal information about you to correct that information, taking into account the nature of the personal information and the purposes of the processing of the personal information.
- **Right to Delete:** You have the right to request that a business delete any personal information about you which the business has collected from you.
- **Right to Opt Out of Selling and Sharing:** You have the right to request that a business not sell your personal information to a third party or share your personal information with a third party for purposes of cross-context behavioral advertising. Opt-out rights can be exercised by contacting privacy@sans.org.
- **Right to Non-Discrimination:** You have the right to not be discriminated against because you exercised any of your CCPA rights.

California residents may make a Request to Know up to twice every 12 months.

If you are a California resident, you may specifically instruct us not sell your Personal Information. SANS does not sell personal data of its customers. If you are a California resident and would like to make a request to exercise your rights under the CCPA, please contact privacy@sans.org. We will respond to verifiable requests received from California residents as required by law. For more information about our privacy practices, you may contact us as set forth in the Section below entitled “Contact Us.”

We will use the following process to verify Requests to Know, Requests to Delete, and Requests to Correct: We will acknowledge receipt of your Consumer Request, verify it using processes required by law, then process and respond to your request as required by law. To verify such requests, we may ask you to provide the following information:

- For a Request to Know categories of personal information which we collect, we will verify your identity to a reasonable degree of certainty by matching at least two data points provided by you against information in our systems which are considered reasonably reliable for the purposes of verifying a consumer’s identity.
- For a Request to Know specific pieces of personal information, Requests to Delete, Requests to Correct, we will verify your identity to a high degree of certainty by

matching at least three pieces of personal information provided by you to personal information maintained in our systems and also by obtaining a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request.

An authorized agent can make a request on a California resident's behalf by providing a power of attorney valid under California law, or providing: (1) proof that the consumer authorized the agent to do so; (2) verification of their own identity with respect to a right to know categories, right to know specific pieces of personal information, or requests to delete which are outlined above; and (3) direct confirmation that the consumer provided the authorized agent permission to submit the request.

For Residents of Virginia

If you are a Virginia resident, the Virginia Consumer Data Protection Act (VCDPA) may grant you the following rights:

- **Right to Access:** You have the right to request whether a business is processing your personal information and to access such personal information.
- **Right to Correction:** You have the right to request that a business correct inaccuracies in your personal information, taking into account the nature of the personal information and our purpose for processing the personal information.
- **Right to Delete:** You have the right to request that a business delete your personal information that was collected about you.
- **Right to Opt Out of Certain Types of Processing.** You have the right to opt out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.
- **Right to Data Portability:** You have the right to obtain a copy of your personal information previously provided to a business in a portable and, if feasible, readily usable format.
- **Right to Non-Discrimination:** You have the right not to be discriminated against by a business for exercising your rights listed above.

Submitting Requests: Right to Access Requests, Right to Correction Requests, Right to Delete Requests, Right to Opt Out of Processing, and Right to Data Portability Requests may be submitted by contacting us at privacy@sans.org.

We will use the following process to verify Right to Access Requests, Right to Correction Requests, Right to Delete Requests, Right to Opt Out of Processing, and Right to Data Portability Requests: We will acknowledge receipt of your request, authenticate it using processes required by law, then process and respond to your request as required by law. To

authenticate such requests, we may ask you to provide additional information as reasonably necessary.

For Residents of Nevada

If you are a Nevada resident, the Nevada Privacy of Information Collected on the Internet from Consumers Act (NPICICA) may grant you the right to request that a business not sell certain kinds of personal information that the business has collected or will collect about you. A “sale” under the NPICICA is the exchange of personal information for monetary consideration by the business to a third party to license or sell the personal information to third parties, with certain exceptions. If you are a Nevada resident and wish to obtain information about SANS’ compliance with Nevada law, please contact us at privacy@sans.org.

Federal Education Rights and Privacy Act (FERPA)

Where applicable, SANS adheres to a U.S. federal law called the Family Educational Rights and Privacy Act (FERPA) that protects student educational records. The Act serves two primary purposes: It gives eligible students more control over their educational records, and it prohibits educational institutions from disclosing “personally identifiable information” in education records without the written consent of an eligible student or in certain other circumstances. To review our full FERPA policy, please visit the [Federal Education Rights Privacy Act Policy](#).

Children’s Personal Information

When SANS collects personal information from or about children under the age of 17, we seek appropriate parental consent to process their information.

SANS products and services are not directed to children under the age of 13. SANS does not knowingly collect any personal information from children under the age of 13, nor does SANS knowingly distribute such information to third parties. If SANS becomes aware that it has received personal information from someone under the age of 13, SANS will take steps to delete such information from its records. If you believe SANS has personal information from individuals under the age of 13, please contact SANS at privacy@sans.org.

Other Important Information

Security

The security of your Personal Information is important to us. Be aware that the internet is a global communications vehicle open to threats, viruses, and intrusions from others, so we cannot

promise - and you should not expect - that we will be able to protect your personal information at all times and in all circumstances.

Contact Us

To make a request or exercise your data privacy rights, if you have a complaint, or if you have any questions or suggestions regarding this Policy or our processing of your personal information, please contact us at privacy@sans.org or at +1 301-654-7267 and request to speak to the Data Privacy Department.

