SANS Security Awareness License Agreement

This LICENSE AGREEMENT ("Agreement") is made and entered into by and between The Escal Institute of Advanced Technologies, Inc. /dba SANS Institute located at 11200 Rockville Pike, Suite 200, North Bethesda, MD, 20852, USA ("**SANS**" or "**Service Provider**") and [CLIENT NAME] (**"Client"**). SANS and Client may be referred to in this Agreement individually as a "Party" and together as the "Parties."

IT IS AGREED BY THE PARTIES:

1. DEFINITIONS

a. **Active User** means a Named User (defined hereafter) who launched, consumed, or activated at least one Learning Activity (defined hereafter) during the relevant 12-month License Term (defined hereafter).

b. **Advanced Cybersecurity Learning Platform (ACLP)** means the training platform owned and operated by SANS. The ACLP is used by SANS and/or SANS clients to manage and deliver training.

c. **Affiliate** means any parent or subsidiary of Client, any entity of which more than fifty percent (50%) of the equity is owned by Client, and/or any individual contractor and agent personnel located in any Client's workspaces. Client Affiliates may not include individuals included on the US Treasury Department's Office of Foreign Asset Control ("OFAC") sanctions list and/or entities located in countries sanctioned by OFAC. https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx.

d. **Applicable Data Protection Law** means all applicable international, federal, state, provincial and local laws, rules, regulations, directives and governmental requirements relating in any way to the privacy, confidentiality or security of Personal Data, including (but not limited to) EU Data Protection Law, the Swiss Federal Data Protection Act (as amended and replaced from time to time); the UK Data Protection Act (as amended and replaced from time to time); the Data Protection Acts of the countries of the European Economic Area ("EEA"), and the Privacy Shield.

e. **Client Materials** means any data or materials, not provided by SANS or its suppliers, that are used in connection with the SANS Advanced Cybersecurity Learning Platform (SANS ACLP) or the SANS Virtual Learning Environment (VLE) or Service Deliverables (defined hereafter), such as technical information and functional specifications, user data, logos, photographs, compilations of facts, artwork, animations, video or audio files, or source materials for any of the foregoing.

f. **Computer Based Training** (**CBT) Materials** means SANS Security Awareness copyrighted training products, each of which are sold separately:

   i. SSA.EndUser Security Awareness Training
   ii. SSA.Developer Security Awareness Training
   iii. SSA.Engineer Security Awareness Training
   iv. SSA.CIP Security Awareness Training
   v. SSA.Healthcare Security Awareness Training

g. **Confidential Information** means any information and materials, including, but not limited to, business or technical data or know-how, customer and prospective customer lists, trade secrets, ideas, concepts, designs, drawings, flow charts, diagrams, methods of operation, computer programs, financials, sales and distribution, marketing, research and development, organizational, policies or practices, portfolio holdings and securities-related information, non-public personal information, 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, which is furnished or revealed by the Discloser (defined hereafter) to the Recipient (defined hereafter). Any abstracts, summaries or compilations are included within the definition of Confidential Information.

h. **Data Controller or Controller** means the natural or legal person, public authority, agency or other body which, alone, or jointly with others, determines the purposes and means of processing of Personal Data (defined hereafter), where the purposes and means of such processing are determined by Union or Member state law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

i. **Data Processor** means a natural or legal person, public authority, agency or other body which processes Personal Data (defined hereafter) on behalf of the Data Controller.

j. **Data Subject** means a natural person whose Personal Data are Processed in the context of this Agreement.

k. **Discloser** means the Party that discloses their Confidential Information to the Recipient (defined hereafter).

l. **Deployment Date** means the date SANS delivers to Client login credentials to access and utilize SANS CBT Materials or SSA.Phishing Service.

m. **EU Data Protection Law** means the EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time) and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC, and as amended and replaced from time to time) and their national implementing legislations.

n. **Europe** means the EEA and Switzerland.

o. **GDPR** means the EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time).

p. **Learning Activity** means any Client Materials delivered by the SANS ACLP, SANS VLE, or Client-supplied Learning Management System (LMS), and/or any item among the CBT Materials that are launched, consumed, or activated by Active Users expressly as part of SANS information security training, SANS security education, SANS security testing and/or SANS security certification products and services, including without limitation to video, audio or other files and documents.

q. **License Term** means from Deployment Date through termination of SANS service(s), i.e., collectively the Initial Term and any Renewal Term(s) as further defined in Section 6.

r. **Named User** means any individual with a user login account permitting such individual to access and use SANS Learning Activity(ies), whether through the SANS ACLP, SANS VLE, or Client-supplied LMS, or the SSA.Phishing Service. Client shall be permitted to identify Client personnel and its Affiliates as Named Users.

s. **Personal Data** means any information relating to an identified or identifiable natural living person ("Data Subject"); 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.

t. **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, or Personal Data transmitted, stored or otherwise Processed.

u. **Processing of Personal Data** (or "Processing/Process") 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.

v. **Recipient** means the Party that receives Confidential Information of the Discloser.

w. **SANS Price Quote** means the document that details the SANS product(s), product information/description, quantities, fees, and License Term, and ordering and payment schedule.

x. **SANS Invoice** means the document that provides an itemized list of all Services (defined herein below) provided by SANS to Client, including the rate, amount, balance due, and payment terms.

y. **Sensitive Data** means any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health, or data concerning a natural person's sex life or sexual orientation, as well as any other type of data that will be considered to be sensitive according to any future revision of EU Data Protection Law.

z. **Service Deliverables** means the items to be delivered to Client in connection with custom services SANS performs pursuant to a separate statement of work, such as consulting reports, on-site training, custom phishing or phishing training templates, SANS ACLP or SANS VLE integration work or SANS ACLP or SANS VLE modifications. Service Deliverables do not include the SANS ACLP or SANS VLE licensed hereunder.

aa. **Sub-Processor** means the entity engaged by the Processor or any further sub-contractor to Process Personal Data on behalf of and under the instructions of the Controller.

bb. **Support Materials** means SANS fact sheets, audio files, videos, Newsletters, Posters, and Screensavers for End-Users.

cc. **User** means an Active User. Client may not exceed the number of Users identified on the SANS Price Quote and under quantity (QTY) on the SANS Invoice.

dd. **Virtual Learning Platform (VLE)** means a training platform owned and operated by SANS. The VLE is used by or for SANS' clients to manage and deliver training.

2. COMPUTER BASED TRAINING (CBT) MATERIALS

a. Subject to Client providing full payment as detailed in the SANS Price Quote, Client is hereby granted a non-exclusive, non-transferable, and non-sublicensable license to permit the Named Users to access and use the CBT Materials as detailed in the SANS Price Quote this Section 2.

b. CBT Materials are limited to no more than the number of Users set forth in this Agreement.

c. Each product line, such as, but not limited to, SSA.EndUser, SSA.Developer, SSA.Engineer, SSA.Healthcare and SSA.CIP, if purchased, will have a separate Active User count, as set forth by the SANS Price Quote and/or SANS Invoice.

d. A Named User will not be counted against Client's total allotment of product line Active Users until the Named User's first viewing of any Learning Activity in a given product line in to one of the following, at which point they become an Active User:

i. SANS' hosting of the CBT Materials for Client on the SANS VLE, which may be updated or changed during the term of this Agreement.
ii. SANS' hosting of the CBT Materials for Client on the SANS ACLP, which may be updated or changed during the term of the agreement.
iii. Client's hosting of the CBT Materials on its own Learning Management System ("**Client LMS**").

e. For the avoidance of doubt, Named Users will not be counted against Client's total allotment of Active Users identified on the SANS Invoice if a user profile is created but the corresponding Named User does not login to the SANS VLE, SANS ACLP or Client LMS to access the SANS CBT Materials.

f. Client agrees to:

i. use the CBT Materials in accordance with the terms of this Agreement;
ii. ensure its Named Users and Active Users comply with the terms of this Agreement and shall be responsible for any Named or Active User's breach of this Agreement;
iii. notify SANS within ten (10) days of any known unauthorized use of Client's account;
iv. not copy, reproduce, distribute, display, modify or create derivative works based upon all or any portion of the CBT Materials and/or Support Materials in any medium, whether printed, electronic or otherwise, without the express written consent of SANS;
v. not sell, resell, rent, or lease the SANS CBT Materials;
vi. not interfere with or disrupt the integrity or performance of the SANS VLE or SANS ACLP service; and
vii. not attempt to gain unauthorized access to the SANS VLE, SANS ACLP, or their related systems or networks.

g. The default delivery language for CBT Materials is English. Additional voice and text translations may be available; unless otherwise specified in this Agreement, SANS reserves the right to add or delete translated languages as CBT Materials are updated.

h. CBT Materials delivered to Client pursuant to the terms of this Agreement may be branded with Client's logo. SANS agrees that it will not use Client's logo for any other use without Client's prior written approval, which approval may be granted or withheld in Client's sole discretion. Client does not receive any additional rights to CBT Materials, outside the terms of this Agreement, as a result of CBT Materials having been branded with Client's logo.

i. Users may view CBT Materials and complete assessments and exams an unlimited number of times during the License Term.

j. Should Client start using the CBT Materials in non-trial and/or non-demo manner, such action shall be deemed as acceptance of the terms and conditions outlined herein and automatic execution of this Agreement.

3. SUPPORT MATERIALS

a. If Client selected Support Materials, subject to Client providing full payment as detailed the SANS Price Quote, Client is hereby granted a non-exclusive, non-transferable, and non-sublicensable license to use the Support Materials for its own internal use as identified in the SANS Price Quote and this Section 3.

b. Support Materials:

i. are provided as digital files only.
ii. are not subject to "per-User" limitations.
iii. may be modified or updated by SANS from time to time.

c. Client agrees to:

i. use the Support Materials in accordance with the terms of the Agreement;
ii. ensure its Named Users and Active Users comply with the terms of this Agreement and shall be responsible for any Named or Active User's breach of this Agreement;
iii. not copy, reproduce, distribute, display, modify, or create derivative works based upon all or any portion of the Support Materials in any medium, whether printed, electronic or otherwise, without the express written consent of SANS;
iv. not attempt to gain unauthorized access to the SANS VLE, SANS ACLP, or their related systems or networks.

e. The default delivery language for Support Materials is English, unless specifically identified otherwise in the SANS Price Quote and SANS Invoice. If Client is eligible to receive Support Materials in more than one language, such option will be indicated in the SANS Price Quote and SANS Invoice at an additional cost.

f. Support Materials delivered to Client pursuant to the terms of this Agreement may be branded with Client's logo. SANS agrees that it will not use Client's logo for any other use without Client's prior written approval, which approval may be granted or withheld in Client's sole discretion. Client does not receive any additional rights to Support Materials, outside the terms of this Agreement, as a result of Support Materials having been branded with Client's logo.

g. Should Client start using the Support Materials in non-trial and/or non-demo manner, such action shall be deemed as acceptance of the terms and conditions outlined herein and automatic execution of this Agreement.

4. SSA.PHISHING SERVICE

a. If Client selected the SANS Phishing Service ("SSA.Phishing Service"), subject to Client providing full payment as detailed in the SANS Price Quote, Client is hereby granted a non-exclusive, non-transferable, and non-sublicensable license to use the SSA.Phishing Service limited to the specifications detailed in the SANS Price Quote and this Section 4. SSA.Phishing Service use is limited to no more than the number of SSA.Phishing Active Users set forth in this Agreement.

b. The SSA.Phishing Service is hosted by SANS for Client on the SANS ACLP and available to Client's designated administrators via password-protected, assigned logins through any Internet-enabled browser.

c. An SSA.Phishing Named User will not be counted against Client's total allotment of SSA.Phishing Active Users until the first email is sent to the SSA.Phishing Named User by the SSA.Phishing Service, at which point the SSA.Phishing Named User becomes an SSA.Phishing Active User.

d. For the avoidance of doubt, SSA.Phishing Named Users will not be counted against Client's total allotment of Active Users in any other product line if a user profile is created, but the corresponding Named User is not sent an email through the SSA.Phishing Service.

e. All Client Materials uploaded by Client to the SSA.Phishing Service remain the sole property of Client or its licensor. Client grants SANS the right to use the Client Materials solely for purposes of performing under this Agreement.

f. Client agrees to:

i. use the SSA.Phishing Service in accordance with the terms of the Agreement and in accordance with the SSA.Phishing Service's user guide and applicable law;
ii. ensure compliance with the terms of this Agreement;
iii. notify SANS within ten (10) days of any known unauthorized use of Client's account;
iv. not reverse engineer the SSA.Phishing Service or associated documentation;
v. not remove or modify any proprietary marking or restrictive legends in the SSA.Phishing Service or documentation;
vi. not access the SSA.Phishing Service or documentation to build a competitive service or product, or copy any feature, function or graphic for competitive purposes.
vii. not sell, resell, rent or lease the SSA.Phishing Service;

viii. not use the SSA.Phishing Service to store or transmit infringing, unsolicited marketing emails, libelous, or otherwise objectionable, unlawful or tortious material, or to store or transmit material in violation of third-party rights;
ix. not interfere with or disrupt the integrity or performance of the SSA.Phishing Service;
x. not attempt to gain unauthorized access to the SSA.Phishing Service or their related systems or networks;
xi. only use the SSA.Phishing Service with its Named and/or Active Users; and
xii. only conduct simulated phishing emails to domains owned by Client, and recipients for whom Client has authorization or expressed consent. Client may not use logos, trademarks, or copyrighted material that Client does not own or is not licensed to use.

g. The default delivery language for the SSA.Phishing Service is English, unless specifically identified otherwise in the SANS Price Quote and SANS Invoice. If Client is eligible to receive the SSA.Phishing Service Materials in more than one language, such option will be indicated on the SANS Price Quote and SANS Invoice at an additional cost.

h. Should Client start using the SSA.Phishing Service in a non-trial and/or non-demo manner, such action shall be deemed as acceptance of the terms and conditions outlined herein and automatic execution of this Agreement.

5. SANS ADVANCED CYBERSECURITY LEARNING PLATFORM (ACLP)

a. Each individual permitted to access or use a component of the SANS ACLP must be assigned a unique user login account and will be considered a Named User. Client may not knowingly permit more than one person to access, use, or share a single user login account to access or use the SANS ACLP.

b. Client must adhere to SANS' reasonable recommendations to ensure system performance, including, but not limited to, recommendations regarding data purging, hosting hardware and infrastructure, and loads per instance. Named User licenses are per-production-instance of the SANS ACLP, and a single Named User license cannot be used on multiple production instances.

c. For a client and their Affiliates with more than 20,000 individuals eligible for SANS training on the ACLP, Named Users allowed in the system is not to exceed two times the number of Active Users in the system.

i. For example, a client has 30,000 individuals eligible for training, but is only training 15,000 Active Users; the number of Named Users in the system is not to exceed 30,000 Named Users.

d. For a client and their Affiliates with less than 20,000 individuals eligible for SANS training on the ACLP, Named Users allowed in the system is not to exceed four times the number of Active Users in the system.

i. For example, a client has 15,000 individuals eligible for training, but is only training 10,000 Active Users, the number of Named Users in the system is not to exceed 40,000 Named Users.

e. SANS represents and warrants that the SANS ACLP can report accurately on the number of Active Users according to the definitions herein. Client agrees to maintain accurate and detailed records of the number of Active Users licensed to use the SANS ACLP. SANS shall have the right to verify the number of Active Users associated with this Agreement.

f. Client may not use the SANS ACLP to: (i) deliver training or manage data on behalf of any other organization; (ii) provide software or content development services to third parties; and/or (iii) deliver training or manage data other than for information security training, information security education, information security testing, or information security certification.

g. Client may not: (i) use, copy, modify, translate, merge or create derivative works of the SANS ACLP, Service Deliverables, documentation, Support Materials or CBT Materials, except as expressly provided in this Agreement; (ii) disable or circumvent any licensing control feature in the SANS ACLP or Service Deliverables; (iii) reverse-engineer, disassemble, or decompile the SANS ACLP or Service Deliverables, or otherwise attempt to access or determine its underlying source code, underlying ideas, underlying user interface techniques or algorithms, or permit any such actions; (iv) distribute, lend, sublicense, rent or lease all or any portion of the SANS ACLP or Service Deliverables, and/or (v) use the SANS ACLP or Service Deliverables on a service bureau or time-share basis or as an application service provider.

6. TERM AND TERMINATION

a. The License Term will begin on Deployment Date for the period of time specified on the SANS Price Quote and SANS Invoice **("Initial Term")** and will automatically renew for successive twelve (12) month terms **("Renewal Terms")** unless cancelled in writing by Client ninety (90) days prior to end of Initial Term or each successive Renewal Term.

b. Client acknowledges and agrees that, to the extent authorized by applicable law, SANS may suspend and ultimately terminate Client's access to the SANS ACLP, SANS VLE, CBT Materials, Support Materials, and/or the SSA.Phishing Service in connection with any:

   i. Material breaches or material violations of this Agreement that have not been cured by Client within (30) days of written notice of such breach or violation;
   ii. Technical or security issues or problems caused by Client that materially impact the business operations of SANS or other SANS clients, whether directly or indirectly, that have not been cured by Client within thirty (30) days of receipt of written notice by either Party of such issues or problem caused by or relating to Client; and/or
   iii. Requests by law enforcement or governmental agencies. SANS will notify Client of such requests if permitted by law.

7. SANS PRICE QUOTE AND SANS INVOICE

a. Client's applicable SSA products, Service Deliverables, number of Users, License Term, and associated fees are set forth in the SANS Price Quote. The items set forth in the SANS Invoice may be updated from time to time by mutual written agreement of the Parties.

b. Client shall choose from the following hosting options, which will be indicated in the SANS Price Quote and SANS Invoice:

   i. CBT Materials hosted by SANS for Client on the SANS VLE and available to Client's Active Users via assigned password-protected logins through any Internet-enabled browser.
   ii. CBT Materials hosted by SANS for Client on the SANS ACLP and available to Client's Active Users via assigned password-protected logins through any Internet-enabled browser.
   iii. CBT Materials hosted by Client on Client's own Learning Management System (Client LMS). SANS will provide Client with reasonable email and telephone support to assist Client during setup and solution deployment.

c. Client may choose to add additional Active Users to its license during the License Term. The unit cost per additional User will be the same as the price paid at the beginning of the License Term. The additional Users' license term will run concurrently with the existing Users' License Term. Adding additional Users to the license will not extend the end date for the License Term. The minimum number of Active Users for additional purchase is:

   i. Two hundred fifty (250) additional Active Users for SSA.EndUser, SSA.Healthcare, and SSA.Phishing
   ii. Four (4) additional Active Users for SSA.Developer
   iii. Twenty (20) additional Active Users for SSA.CIP and SSA.Engineer

8. PAYMENT TERMS

a. Client will be invoiced by SANS for one hundred percent (100%) of the agreed total fee for CBT Materials, Support Materials, and/or SSA.Phishing Service as selected by Client.

b. Payment must be completed in full prior to Deployment Date. License Term will begin on the Deployment Date.

c. Payment for Renewal Term(s) shall be received in full prior to the end of Initial Term or each successive Renewal Term.

9. NON-DISCLOSURE

a. Obligation of Confidentiality and Limited Use. The Parties recognize and acknowledge that this Agreement creates a confidential relationship between Parties. The Recipient will prevent the disclosure and protect the confidentiality of the Discloser's Confidential Information during the Term of this Agreement and for three years 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 Discloser's Confidential Information solely in connection with this Agreement. The Recipient will not use the Discloser's Confidential Information for the benefit of, or transmit the Discloser's Confidential Information to, any third party without first obtaining the express written consent of the Discloser. The Recipient shall not copy, distribute or disclose this Agreement and the Discloser's Confidential Information except to those employees, officers, directors, subcontractors, agents or Affiliates of the Recipient ("**Representatives**") who have a need to know such Confidential Information as required in connection with this Agreement, provided such Representatives are advised of and agree to abide by the confidentiality obligations set forth in this Agreement. Compliance by Representatives with the confidentiality and use obligations in this Agreement will remain the responsibility of Recipient and both Recipient and Representatives shall be liable for any breach of this Agreement by Representatives. Unless otherwise permitted in this Agreement, neither Party will make or issue, or cause to be made or issued, any announcement or statement regarding activities under this Agreement for dissemination to the general public or any third party without the prior written consent of the other Party.

In the unlikely event SANS is provided access to any portfolio holdings or securities-related information, SANS agrees not to trade on any such information, and to make best efforts to ensure that its employees, agents, and subcontractors do not trade on such information.

Nothing contained in this Agreement will be construed as granting or conferring any rights by license or otherwise to either Party's Confidential Information other than as expressly provided in this Agreement.

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

i. was or becomes generally available to the public through no breach of this Agreement by the Recipient or Recipient's Representatives;
ii. was rightfully in the Recipient's or its Representatives' possession prior to receipt from the Discloser;
iii. becomes rightfully available to the Recipient or its Representatives from a source other than the Discloser who is free to lawfully disclose such information to the Recipient;
iv. is approved for release by written agreement of Discloser; or
v. is independently developed by the Recipient or its Representatives, as evidenced by written records, without the use of the Discloser's Confidential Information.

Confidential Information shall not be deemed to be in the public domain merely because any part of the Confidential Information is embodied in general disclosures or because individual features, components or combinations thereof are now or become known to the public.

If Confidential Information is required to be disclosed by the Recipient by a governmental agency or law, such Confidential Information may be disclosed pursuant to such requirement so long as the Recipient provides the Discloser with written notice of the required disclosure promptly upon receipt of notice, to the extent such notice is permitted by law, and cooperates with the Discloser in any efforts to limit the nature and scope of such required disclosure.

c. Return of Confidential Information. Discloser shall maintain all rights to their Confidential Information. Upon termination of this Agreement, at Discloser's request, Recipient will destroy or return to Recipient all Discloser Confidential Information in its possession or control and provide written certification of compliance thereof. Notwithstanding the above, Recipient may maintain a single copy of the Confidential Information in Recipient's legal archives for the sole purpose of determining the scope of its rights and obligations incurred under this Agreement.

d. Unauthorized Access. Recipient agrees to take appropriate actions to address incidents of unauthorized access to Discloser's Confidential Information, including notification to Disclosure of any such incident. Any such notification will be within ten (10) days from the date that Recipient is made aware of such unauthorized access except as otherwise required by applicable law.

10. INTELLECTUAL PROPERTY

a. Client acknowledges that SANS' ACLP, VLE, CBT Materials, Support Materials, and SSA.Phishing Service (the "**Services**") are copyrighted and/or otherwise consist of data, concepts, technology, and intellectual property proprietary to SANS and are the sole property of SANS. Except as expressly stated herein, this Agreement does not grant Client any rights to, under or in, any patents, copyright, database right, trade secrets, trade names, trademarks (whether registered or unregistered), or any other rights or licenses in respect of the Services.

b. SANS acknowledges that Client's logo is the sole property of Client. Unless otherwise permitted herein, SANS shall not, except for SANS' use of such property as granted under Sections 2, 3, and 4 hereof, use Client's name, trademarks, service marks, logos, trade names and/or branding in any commercial, marketing, publicity or other manner, in connection with products and/or Services under this Agreement, without Client's prior written permission, which permission may be granted or denied in Client's sole discretion.

11. REPRESENTATIONS AND WARRANTIES

a. SANS represents and warrants to Client:

i. it has full right and power to enter into this Agreement;
ii. it is duly organized and in good standing under the laws of the jurisdiction in which it is organized;
iii. it is not currently the subject of voluntary or involuntary petition in bankruptcy, is not currently contemplating filing any such voluntary provision, and is not aware of any claim for the filing of an involuntary petition;

iv. it will perform with reasonable care and skill;
v. it will perform in a professional, diligent, timely and competent manner, consistent with industry standards and commercial practices;
vi. its intellectual property will not infringe any known intellectual property rights of any third party or violate any federal, state or municipal laws;
vii. industry best practices, including backing up of data, use of redundant hardware and storage devices, and protections from viruses and other malicious attacks, will be used to protect Client's Confidential Information.

The warranties extended herein by SANS are in lieu of all other warranties, expressed or implied.

12. INDEMNIFICATION

a. SANS agrees to defend, indemnify, and hold harmless Client, and their respective successors, assigns, employees, officers, directors and agents (each a "**Client Indemnified Party**" and collectively the "**Client Indemnified Parties**") from and against any and all claims, losses, liabilities, damages, and costs, including reasonable attorney fees and expenses brought against or suffered by a Client Indemnified Party, alleging that the CBT Materials, Support Materials, or SSA.Phishing Service provided pursuant to this Agreement infringe any known patent, copyright, trademark, trade secret or other intellectual property interest in any country, provided that Client:

i. Promptly notifies SANS in writing of the claim; and
ii. Allows SANS to control, and cooperates with SANS in, the defense and any related settlement.

b. In the event of an infringement, SANS shall in its sole discretion, at no additional charge to Client, promptly replace, in whole or in part, the infringing products and/or Services with a substantially compatible and functionally equivalent product, or modify them to avoid the infringement. Should it be commercially unreasonable to make the products and/or Services non-infringing, SANS shall accept the return of the infringing products and/or Services and refund to Client the applicable fees paid relative to the infringing products and/or Services.

c. Specifically regarding the SSA.Phishing Service, Client agrees to defend, indemnify, and hold harmless SANS, and their respective successors, assigns, employees, officers, directors and agents (each a "**SANS Indemnified Party**" and collectively the "**SANS Indemnified Parties**") from and against any and all claims, losses, liabilities, damages, and costs, including reasonable attorney fees and expenses brought against or suffered by a SANS Indemnified Party, alleging that Client's intellectual property used in connection with this Agreement infringe any known patent, copyright, trademark, trade secret or other intellectual property interest in any country, provided that SANS:

i. Promptly notifies Client in writing of the claim; and
ii. Allows Client to control, and cooperates with Client in, the defense and any related settlement.

13. LIMITATION ON SANS' LIABILITY

EXCEPT AS PROVIDED IN SECTION 12, INDEMNIFICATION, IN NO EVENT SHALL SANS, ITS AFFILIATES OR ANY OF THEIR RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS LIABILITY TO CLIENT IN ANY MANNER ARISING UNDER THIS AGREEMENT EXCEED AN AMOUNT EQUAL TO THE TOTAL FEES RECEIVED BY SANS FOR PRODUCTS AND/OR SERVICES UNDER THIS AGREEMENT DURING THE 12-MONTH PERIOD IMMEDIATELY PRECEDING THE DATE WHEN CAUSE OF ACTION ARISES, INCLUDING ATTORNEY FEES.

14. INSURANCE

a. SANS shall, during the term of this Agreement, maintain appropriate insurance, including:

i. Worker's Compensation insurance in an amount satisfying applicable laws, and employers' liability insurance in an amount not less than $1,000,000 per occurrence;
ii. Commercial General Liability insurance in an amount not less than $1,000,000 per occurrence;
iii. Umbrella insurance in an amount not less than $15,000,000 per occurrence.
iv. Errors & Omissions insurance, including Professional Liability, Data Privacy and Network Security Liability, and Media Liability in an amount not less than $1,000,000 per occurrence.

15. INDEPENDENT CONTRACTOR

SANS acknowledges that any products and/or Services rendered under this Agreement shall be solely as an independent contractor. SANS shall not enter into any agreement or commitment on behalf of Client. SANS further acknowledges that it is not

considered an affiliate or subsidiary of Client and is not entitled to any Client employment rights or benefits. SANS shall not be subject to Client's control or direction in the manner of its performance under this Agreement. It is expressly understood that this undertaking is not a joint venture.

16. GOVERNING LAW

This Agreement and any disputes arising hereunder shall be interpreted and adjudicated in accordance with the laws of the State of Maryland, USA (without regard to the choice of law principles of any jurisdiction).

17. MEDIATION

Any dispute arising between the Parties, in connection with this Agreement which is not settled to the mutual satisfaction of the Parties within thirty (30) business days from the date that either Party informs the other in writing that such dispute exists, shall prior to litigation, be first mediated in a location to be agreed to by the Parties. The fees and the costs shall be borne equally by the Parties. The foregoing shall not preclude either Party from seeking equitable relief in addition to all other remedies available at any time in the event of a breach of obligations under Section 9, Non-Disclosure.

18. SEVERABILITY

In the event that any provision of this Agreement becomes or is declared by a court of competent jurisdiction to be illegal, unenforceable or void, this Agreement shall continue in full force and effect without said provision, provided that no such severance shall be effective if it materially changes the economic benefit of this Agreement to either Party.

19. DEFAULT

Failure to honor the material terms and conditions contained in this Agreement on the part of either Party shall constitute a default under this Agreement. The non-defaulting party shall give written notice of default via Certified US Mail, return receipt requested, or overnight carrier of the specific nature of the default and allowing the defaulting party thirty (30) business days from receipt of the written notice to cure the default. Should the defaulting party fail to cure the default within the specified time period, the non-defaulting party thereafter shall have the right to declare this Agreement void and terminate the remaining obligations under this Agreement, except those that are intended by their terms to survive. In the event of default by SANS, it will provide Client a prorated refund for fees previously paid and unused for the period starting on the date of termination to the end of the License Term. For purposes of clarity, the foregoing is not intended to in any way limit Client's rights in law or equity with respect to such default/breach or otherwise.

20. WAIVER

The failure of either Party to exercise or enforce any right or provision of this Agreement shall not constitute a waiver of such right or provision.

21. ASSIGNMENT

Neither Party hereto may assign this Agreement or its rights and obligations under this Agreement without the written consent of the other Party, which consent will not be unreasonably withheld, provided, however, that SANS' consent shall not be withheld for any complete or partial assignment made by, between or among entities within Client's worldwide enterprise, or if such assignment or transfer is made as the result of (i) a corporate merger; (ii) a sale of all or substantially all of the corporate assets of such entity; (iii) a sale of a controlling interest in such entities' corporate stock; (iv) a corporate reorganization; or (v) as a result of a corporate name change. No additional fees or costs shall be associated with any assignment permitted hereunder. In the event an entity member of Client's enterprise shall become an independent entity, Client may assign to the former entity member of Client's enterprise the number of licenses then in use on the same terms and conditions as are contained in this Agreement. Neither Client nor the former entity member of Client's enterprise shall owe any further remuneration for licenses already paid for, and there shall be no transfer fees associated with such assignment. Additional licenses, if any are needed by the former entity member of Client's enterprise, will be available to the former entity member of Client's enterprise at the same prices available to Client under this Agreement, for a period of one (1) year from the date of assignment.

22. THIRD PARTY BENEFICIARY RIGHTS

Nothing in this Agreement shall benefit or create any right or cause of action in or on behalf of any person or entity other than Client and SANS.

23. SURVIVAL

Sections 6, 9, 10, 11, 12, 13, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, and 27 shall survive any termination of this Agreement.

24. OTHER PROVISIONS

a. SANS will not enter Client's premises to perform Services under this Agreement. Client is fully responsible for deployment of the service in its organization. SANS will only support such deployment remotely.
b. SANS shall not offer or give a gratuity of any type to any Client employee or agent.
c. Client will be eligible to participate in SANS' Client Reference Program which may include, but is not limited to, participation in client case studies, press releases, collateral, and opportunities with media and industry analysts. SANS is permitted to use Client's name in lists with other clients. However, SANS shall not use Client's name in any other advertising material (including, without limitation, online or print-based advertisements) without advance written authorization from Client.
d. For purposes of further enhancing CBT Materials, Support Materials, SANS ACLP, and SANS VLE, anonymous, non-company specific, and non-personally identifiable information regarding Client's training usage may be collected and, after being aggregated with all training usage information, made a part of CBT Materials, Support Materials, SANS ACLP, and SANS VLE.
e. The Convention on Contracts for the International Sale of Goods, and the Virginia Uniform Computer Information Transactions Act do not apply.

25. EUROPEAN DATA PROTECTION

a. The SANS Institute has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Privacy Shield Framework. SANS shall, during the term of this Agreement, continue to adhere to the EU-U.S. Privacy Shield Framework, as applicable. Without limiting the foregoing, SANS acknowledges that the General Data Protection Regulation (**GDPR**) (Regulation (EU) 2016/679 became effective on 25 May 2018. SANS shall, as applicable to the Services delivered, be compliant and remain compliant for the Term of this Agreement. In the event SANS makes a determination that (1) it can no longer meet its obligations under the EU-U.S. Privacy Shield Framework; and/or (2) it can no longer meet its obligations under the GDPR, it will notify the Client within fifteen (15) business days of making such a determination.

b. To the extent a Data Processing Agreement (DPA) for SANS' Processing of Personal Data, within the scope of GDPR, directly applies to SANS' provision of Services under this Agreement, attached hereto as Exhibit B is a DPA that forms part of this Agreement. If the DPA forms part of this Agreement, the DPA is effective upon the effective date of this Agreement.

c. For the avoidance of doubt, the Processing of Personal Data under the DPA is governed by England and Wales. Any disputes between the Parties relating to the Processing of Personal Data under the DPA will be subject to the exclusive jurisdiction of the courts in England and Wales.

26. NOTICE

Unless otherwise addressed in the DPA, any required notice shall be delivered to the Parties' respective addresses set forth on the SANS Invoice.

27. ENTIRE AGREEMENT; PRECEDENCE; AMENDMENT

a. This Agreement, together with any proposals, statements of work, SANS Price Quote, and/or SANS Invoice, referencing Client's procurement of SANS Security Awareness, contains the entire understanding and agreement between SANS and Client and replaces and extinguishes all prior agreements and understandings as to the subject matter hereof. This Agreement shall become binding upon execution by both Parties or by SANS accepting payment from Client.

b. To the extent the terms and conditions are inconsistent or conflict, the order of precedence is: this License Agreement; statements of work; SANS Price Quote; SANS Invoice; and lastly, any proposals. It is understood and agreed between Parties that a Client's Purchase Order (PO) is for facilitating invoicing and payment only and that any terms included on a PO are hereby rejected. For the avoidance of doubt, if the DPA attached hereto as Exhibit B applies as specified in Section 25.b, the Parties agree that the terms of Exhibit B supersede and replace any conflicting privacy and data protection terms contained in the Principal Agreement pertaining to the Processing of Personal Data subject to EU Data Protection Law.

c. This Agreement may not be amended without the specific written consent of both Parties. Any amendments incorporated in and made a part of this Agreement, must address, with specific reference, the Section(s) of this Agreement that the Parties agree to modify.

Exhibit A

Client Maintenance and Support

1. **Client Support** means response or assistance provided to Client by SANS for items that are not an Error (defined hereafter). Client Support will be provided as indicated on SANS Price Quote and as set forth in Table C3. Help Desk support can be accessed by emailing traininghelp@sans.org.
2. **Designated Contacts** means the individuals designated by Client and agreed to by SANS who are authorized to contact SANS' client maintenance staff and who will coordinate all of Client's Error submissions and maintenance requests.
3. **Error** means a reproducible defect in the SANS ACLP, which causes the SANS ACLP not to operate substantially in accordance with SANS' published documentation.
4. **Maintenance Release** means an update to an existing version of the SANS ACLP containing Error corrections or minor functionality enhancements. A Maintenance Release is designated as a numbered service pack for the current version, with no change in the version number. For example, Version 7 service pack 4 will be referenced as "7.4".
5. **New Version Release** means a new version of the CBT Materials, Support Materials, SSA.Phishing Service, or SANS ACLP containing new features or enhancements to functionality. A New Version Release for the SANS ACLP is designated by an increase in the version number, e.g., from 2.5 to 2.6 or 3.0.
6. **Resolution Effort** means the efforts SANS will use to resolve an Error. SANS' Resolution Efforts depend on the severity of the Error. For each level of severity, Resolution Efforts shall be as set forth in Table C2.
7. **Response Time** means the period of time from when SANS receives an Error notice until SANS contacts the Designated Contact to begin Resolution Efforts. SANS' Response Time depends on the severity of the Error. For each level of severity, SANS' Response Time shall be as set forth in Table C1. *Response Time does not include the time required to resolve and/or deliver an Error correction.*

Response Times:

Table C1	
Severity Level	Initial Response
P-0	1 hour
P-1	4 hours
P-2	8 hours
P-3	2 days

Table C2		
Severity Level	Security Level Description	SANS Resolution Efforts
P-0	Complete Production Outage • Any authorized Primary production site is inaccessible and cannot be used	SANS will use commercially reasonable best efforts to assist client to restore the production instance to full functionality, unless the outage is caused by an infrastructure failure, in which case SANS will provide reasonable support during the restoration of service.
P-1	Production environment does not function • No workaround is available • Critical and significant number of users are affected; and • There is a critical business impact	SANS will use commercially reasonable best efforts to work on the issue as a critical priority and work towards providing a workaround solution, a hot fix or schedule the fix for a roll up patch dependent on the impact and nature of the issue.
P-2	Production environment is operational • A workaround is available • Significant number of users are affected; and • There is a major business impact	SANS will triage and work on the issue and work towards providing a workaround solution or schedule the fix for a roll up patch, maintenance pack or service pack, dependent on the impact and nature of the issue.
P-3	Environment is operational • Minor application issue; or • Cosmetic issue; or • Documentation questions; or • Product feedback or enhancement requests	SANS will identify a potential future delivery date in a future release

Table C3							
Standard Service		Standard Plus Service		Program Service		Enterprise Service	
Channel	Response time	Channel	Response time	Channel	Response time	Channel	Response time
Help Desk	24 Hours during normal business hours	Help Desk	24 Hours during normal business hours	Help Desk	8 Hours during normal business hours	Help Desk	Same Day during normal business hours
				Client Success Manager	As detailed in client project plan or otherwise available	Client Success Manager	As detailed in client project plan or otherwise available

Exhibit B

To the extent a Data Processing Agreement (DPA) for the Processing of Personal Data of Data Subjects subject to GDPR directly applies to SANS' provision of Services under the License Agreement, then (i) this DPA forms part of the License Agreement, and (ii) this DPA is effective upon the effective date of the License Agreement.

Data Processing Agreement

Whereas:

A. Client and Service Provider have entered into a written services agreement relative to Client's procurement of Service Provider's SANS Security Awareness training (the "License Agreement" or "Principal Agreement") which involves Processing of Personal Data of Data Subjects subject to EU Data Protection Law in the context of the Services specified in the Principal Agreement (the "Services").

B. Specific to the Principal Agreement, the Parties have agreed to enter into this Data Processing Agreement ("DPA") which shall govern the Processing of Personal Data of Data Subjects subject to EU Data Protection Law in the context of the Services.

NOW, THEREFORE, the Parties agree as follows:

A. This DPA regulates the Processing of Personal Data of Data Subjects subject to EU Data Protection Law for the Purposes (as defined in Appendix 1 below) by the Parties in the context of the Services.

B. The Parties agree that the terms as set out below supersede and replace any conflicting privacy and data protection terms contained in the Principal Agreement pertaining to the Processing of Personal Data subject to EU Data Protection Law.

C. Appendices 1 and 2 form an integral part of this DPA.

D. Except as modified below, the terms of the Principal Agreement remain in full force and effect.

1. **Definitions**.

Capitalized terms not otherwise defined herein have the meaning given to them in the Principal Agreement.

2. **Roles of the Parties.**

Client and Service Provider agree that:

2.1. in the context of this DPA, Client acts as Controller, and appoints Service Provider as Processor for the Processing of Personal Data for providing the Services. In that context, Client, as Controller, has the sole and exclusive authority to, consistent with the Principal Agreement, determine the purposes and means of the Processing of Personal Data that are disclosed to and collected by Service Provider. Service Provider will Process Personal Data (i) only on behalf and for the benefit of Client, and (ii) only to carry out its obligations under the Principal Agreement as implemented and to the extent required by each individual statement of work and/or Client's written instructions. Service Provider shall not share, transfer, transmit, disclose or otherwise provide access to or make available any Personal Data to any third party unless Client has authorized Service Provider to do so in writing.

2.2. should any person or authority conclude, deem, or assert that Service Provider is a joint Controller with Client, then the Parties agree that Client would maintain the sole and exclusive authority for interactions with the related Data Subjects, including and especially related to Articles 13 and 14 of the EU Data Protection Law.

3. **Service Provider's obligations**.

Service Provider agrees and warrants that it will:

3.1. notify Client, when any law or legal requirement prevents Service Provider (1) from fulfilling its obligations under this DPA or EU Data Protection Law, and/or (2) from complying with the instructions received from Client, via this DPA, unless such notification is prohibited on important grounds of public interest. In both situations, Client is entitled to (i) suspend the Processing of Personal Data by Service Provider; (ii) terminate any further Personal Data Processing; and (iii) terminate this DPA, if doing so is required to comply with Applicable Data Protection Law.

3.2. within 48 (forty-eight) hours inform Client, in writing, as applicable to the Services and related to: (i) any Data Subjects' requests to their rights of (a) access, (b) rectification, (c) erasure, (d) data portability, (e) restriction of Processing, (f) objection to the Processing; and (g) not being subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them; (ii) any request or complaint received from Client, employees, or from any other individual related to this DPA; (iii) any question, complaint, investigation or other inquiries from Data Protection Authorities; and (iv) any public authority of whatever jurisdiction requesting disclosure of or information about the Personal Data that are Processed by Service Provider. Service Provider agrees and warrants that it will provide Client with a copy of any such requests within 48 (forty-eight) hours and that it will respond to such requests only in accordance with Client's prior written authorization and instructions. Taking into account the nature of the Processing, Service Provider will assist Client, by appropriate technical and organizational measures, insofar as this is possible, in fulfilling its obligations to respond to such requests.

3.3. cooperate with and assist Client to comply with and fulfill it its own obligations under Applicable Data Protection Law and this DPA, including: complying with Data Subjects' requests to exercise their rights; replying to complaints from Data Subjects; replying to investigations and inquiries from supervisory authorities; and conducting data protection impact assessments and prior consultations with supervisory authorities.

3.4. upon termination of the Principal Agreement or upon request by Client (i) delete or return Personal Data, and (ii) comply with Client request to delete existing copies unless EU or EU Member State law requires storage of the Personal Data (in which case Service Provider will protect the confidentiality of the Personal Data, will not actively Process the Personal Data anymore, and will continue to comply with this DPA).

4. **Security of the Processing, Confidentiality, and Personal Data Breach Notification**.

Service Provider agrees and warrants that:

4.1. it has implemented and maintains a comprehensive written information security program that complies with EU Data Protection Law and Appendix 2 of this DPA, including appropriate technical and organizational measures to ensure a level of security appropriate to the risk, which includes, at a minimum, the security measures listed in Appendix 2 and as appropriate: (a) the pseudonymization and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of Processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing of Personal Data. In assessing the appropriate level of security, Service Provider must take into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing of Personal Data, as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects and the risks that are presented by the Processing of Personal Data, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed ("Information Security Program").

4.2. Service Provider's Information Security Program must, among other things, include regular testing or otherwise monitoring of the effectiveness of Service Provider's information safeguards. Service Provider undertakes to notify Client of any technical, operational, organizational or other change having a material impact on the security, confidentiality or protection of Personal Data, no less than 15 (fifteen) working days prior to implementing any such

change. Service Provider agrees to submit its Information Security Program to the Data Protection and Security Audit provided under Clause 7.

4.3. Service Provider must take steps to ensure that any person acting under its authority who has access to Personal Data is only granted access to Personal Data on a need-to-know basis, is subject to a duly enforceable contractual or statutory confidentiality obligation, and only Processes Personal Data in accordance with Client instructions.

4.4. as applicable to the provision of Services under this DPA, Service Provider will inform Client, in writing, without undue delay, and no later than 48 (forty-eight) hours after having become aware of a Personal Data Breach. Such notice will summarize in reasonable detail the effect on Client, if known, of the Personal Data Breach and the corrective action taken or to be taken by Service Provider. Service Provider shall assist Client in complying with its own obligations under Applicable Data Protection Law to include the notification of such Personal Data Breach. Service Provider will (i) promptly take all necessary corrective actions; (ii) cooperate fully with Client in all reasonable and lawful efforts to prevent, mitigate or rectify the effects of such Personal Data Breach; and (iii) be responsible for the costs and expenses associated with the performance of its obligations described in this paragraph, unless such Personal Data Breach is caused by the acts or omissions of Client.

4.5. except to the extent prohibited by applicable legal, regulatory, or law enforcement requirements, Service Provider must obtain the approval of Client, prior to the publication or communication of any filings, communications, notices, press releases, or reports related to such Personal Data Breach that expressly mention Client or its Affiliates. Service Provider acknowledges and agrees that a violation of this clause, or the occurrence of such Personal Data Breach, may cause immediate and irreparable harm to Client for which money damages may not constitute an adequate remedy. Therefore, Service Provider agrees that Client may seek injunctive or other equitable relief for any such violation or incident, in addition to its remedies at law, without proof of actual damages.

5. **International data transfers**.

5.1. Service Provider must not transfer Personal Data outside the country to which Client originally delivered it to Service Provider for Processing (or, if it was originally delivered to a location inside the EEA, outside the EEA) without the explicit written consent of Client. For the avoidance of doubt, as agreed between the Parties, this DPA serves as the explicit written consent of Client for Service Provider to transfer Personal Data to the United States for Processing where Service Provider maintains its certification with the EU-U.S./Swiss-U.S. Privacy Shield Framework.

5.2. Service Provider agrees and warrants that it is prohibited from transferring Personal Data that is subject to EU Data Protection Law outside of Europe except if it obtains the explicit written consent of Client and provided that the Personal Data are transferred to a country which has been considered to provide an adequate level of protection under EU Data Protection Law or to a data recipient which has implemented adequate safeguards under EU Data Protection Law such as approved Binding Corporate Rules, Standard Contractual Clauses, or the EU-U.S./Swiss-U.S. Privacy Shield Frameworks. For the avoidance of doubt, as agreed between the Parties, this DPA serves as the explicit written consent of Client for Service Provider to transfer Personal Data to the United States where Service Provider maintains its certification with the EU-U.S./Swiss-U.S. Privacy Shield Framework.

5.3. In the context of the Service, Client agrees that Service Provider transfers or stores Personal Data Processed on behalf of Client in the United States as necessary to perform Services on behalf of Client. Service Provider agrees to protect Personal Data in the United States in compliance with Applicable Data Protection Law and this DPA; Service Provider will not use the Personal Data transferred to the United States for its own purposes.

5.4. Absent the adequacy finding or adequate safeguards referred to in Clause 5.2, the Parties will execute Standard Contractual Clauses. The Standard Contractual Clauses will apply to Personal Data Processed by Service Provider in the context of the Services that are transferred outside of Europe, either directly or via an onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for Personal Data under EU Data Protection Law or to a recipient which has not implemented adequate safeguards under EU Data Protection Law.

For the avoidance of doubt, at the present time, Standard Contractual Clauses are not necessary as Service Provider is not absent the adequacy findings per Section 5.2.

6. **Service Provider's Sub-Processing**.
   6.1. Service Provider has appointed Sub-Processors to Process Personal Data in the context of the Services specified in the Principal Agreement. Service Provider represents and warrants that such Sub-Processors have each entered into binding written agreements with Service Provider that are substantially the same as those that are imposed on Service Provider under this DPA. Upon request, Service Provider will provide a list of its Sub-Processors.
   6.2. Service Provider shall inform Client of any intended changes concerning the addition or replacement of Sub-Processors, and if Client reasonably objects in writing to such addition or replacement within 30 days of receipt of such notification from Service Provider, the Parties shall discuss in good faith Client's concerns and Service Provider shall use reasonable efforts to propose a commercially reasonable change to address Client's concerns. If Client and Service Provider are unable to find a mutually acceptable solution to address Client's concerns, then Client acknowledges and agrees that its sole remedy is to terminate the Principal Agreement for convenience (not breach) in respect of those affected Services on not less than 30 days' notice in writing.
   6.3. Prior to any Sub-Processing, Service Provider must carry out adequate due diligence to ensure that the Sub-Processor is capable of providing Personal Data with at least the same level of protection for the Processing of Personal Data and the same obligations on the Sub-Processor as are imposed on Service Provider under this DPA.
   6.4. Service Provider will provide Client with the necessary information to help verify the Sub-Processor's compliance with its data protection obligations.
   6.5. Service Provider shall remain fully liable towards Client for the performance of any and all Sub-Processor obligations under this DPA.

7. **Data Protection and Security Audit.**
   7.1. Upon request by Client and subject to reasonable discretion, Service Provider will make available to Client information necessary to demonstrate compliance with its obligations under this DPA, and allow Client (or an inspection body composed of independent members mutually selected by the Parties, and which possess the required professional qualifications) to audit and review Service Provider's Information Security Program, data processing facilities, and data protection compliance program to verify compliance with this DPA and Applicable Data Protection Law ("Data Protection and Security Audit").
   7.2. The Parties will mutually agree upon the scope, timing, and duration of the audit, and if necessary on an independent third-party auditor, in which case Service Provider will make available to Client the result of the audit. Service Provider agrees to fully cooperate with such Data Protection and Security Audit and implement all commercially reasonable changes to its Information Security Program, data processing facilities, and data protection compliance program that, as a result of the Data Protection and Security Audit, are required to ensure Service Provider's compliance with this DPA and Applicable Data Protection Law.
   7.3. Service Provider's failure to allow or cooperate with a Data Protection and Security Audit or implement any legally required changes to the information security program shall entitle Client to: (i) suspend the Processing of Personal Data by Service Provider; (ii) terminate any further Personal Data Processing; and (iii) terminate this DPA, if doing so is required to comply with this DPA and Applicable Data Protection Law.

8. **Liability Towards Data Subject.** The Parties agree that they will be held liable for violations of EU Data Protection Law towards Data Subjects as follows:
   8.1. Service Provider will be liable for the damage caused by the Processing only where it has not complied with obligations of EU Data Protection Law specifically directed to Processors.

8.2. Client will be liable for the damage caused by the Processing only where it has not complied with obligations of EU Data Protection Law specifically directed to Controllers.

8.3. Client and/or Service Provider shall be exempt from liability under this Section 8 if it proves that it is not in any way responsible for the event giving rise to the damage.

9. **Applicable Law and Jurisdiction**. The Processing of Personal Data under this DPA is governed by England and Wales. Any disputes between the Parties relating to the Processing of Personal Data under this DPA will be subject to the exclusive jurisdiction of the courts in England and Wales.

10. **Modification of this Data Protection Agreement**. This DPA may only be modified by a written amendment signed by each of the Parties.

11. **Termination.** The Parties agree that this DPA is terminated upon the termination of the Principal Agreement pursuant to which Service Provider obtained Personal Data from Client.

12. **Notices.** Except as provided below, notices provided under this DPA must be in writing and sent by facsimile or certified mail, return receipt requested or sent electronically to the email addresses listed below.

Notices to Service Provider must be sent to:
The Escal Institute of Advanced Technologies, Inc. / dba SANS Institute
ATTN: Contracts
11200 Rockville Pike, Suite 200
North Bethesda, MD 20852
FAX: 301-951-0140
EMAIL: ssagdprprivacy@sans.org

Notices to Client must be sent to:

Company Name: _____

ATTN:_____

Address:_____

Address: _____

FAX: _____

Email: _____

With respect to notice pursuant to Clause 4.4 hereof, notice must be made to:

Client POC: _____

Client POC email address:_____

13. **Invalidity and Severability.** If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such provision shall not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

REMAINDER OF PAGE INTENTIONALLY BLANK

EXHIBIT B - APPENDIX 1: Description of the Processing activities

This Appendix 1 describes the Processing by Service Provider under the DPA.

Subject-matter of the Processing

Service Provider delivers Commercial Off The Shelf (COTS) computer-based training videos by Client assigning the training to their personnel through a learner platform. Service Provider receives, from Client, information regarding their personnel to be assigned training to include: (i) unique learner number, (ii) first name, (iii) last name, (iv) email address; (v) optional additional information about learners provided by Client admins; there are fixed fields and user-defined fields; and (vi) direction when to launch course. The learner platform then launches the course, allows for language selection, and maintains progress and completion information (launch date, time spent, progress, score, and satisfaction). Information relating to the Client learner's launch and progress remains in the learner platform for the duration of the Principal Agreement.

Nature and Purpose of the Processing

Service Provider will Process Personal Data for the purpose of providing the Services, as described in this DPA and the Principal Agreement. Service Provider provides computer based training videos as outlined above.

Types of Personal Data (including Sensitive Data)

Contact details (unique learner number, first name, last name, and email address)

Optional additional information about learners provided by Client admins; there are fixed fields and user-defined fields

System access/usage/authorization data

Categories of Data Subjects

Client Employees

Duration of the Processing

Service Provider will Process Personal Data only for as long as necessary to provide the Services and as permitted under the Principal Agreement and this DPA.

EXHIBIT B - APPENDIX 2: List of Security Measures

The Service Provider will, as a minimum, implement the following types of security measures:

1. Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed, include:

- Establishing security areas, restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers etc.);
- Security staff, janitors;
- Surveillance facilities, video/CCTV monitor, alarm system;
- Securing decentralized data processing equipment and personal computers.

2. Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Creation of **one** master record per user, user master data procedures, per data processing environment;
- Encryption of archived data media.

3. Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, include:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access Personal Data without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure;
- Encryption.

4. Disclosure control

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include:

- Encryption/tunneling;
- Logging;
- Transport security.

5. Entry control

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

- Logging and reporting systems;
- Audit trails and documentation.

6. Control of instructions

Technical and organizational measures to ensure that Personal Data are processed solely in accordance with the Instructions of the Controller include:

- Unambiguous wording of the contract;
- Formal commissioning (request form);
- Criteria for selecting the Processor.

7. Availability control

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include:

- Backup procedures;
- Mirroring of hard disks (e.g. RAID technology);
- Uninterruptible power supply (UPS);
- Remote storage;
- Anti-virus/firewall systems;
- Disaster recovery plan.

8. Separation control

Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately include:

- Separation of databases;
- “Internal client” concept / limitation of use;
- Segregation of functions (production/testing);
- Procedures for storage, amendment, deletion, transmission of data for different purposes.