ARMOR CLOUD SERVICES SCHEDULE

This Armor Cloud Services Schedule ("**Schedule**"), together with the Armor Master Services Agreement ("**MSA**") and the Order signed by you for Services falling within the scope of this Schedule, govern Armor's provision of the Services (as defined below) to you. Capitalized terms not defined below have the meaning set forth in the MSA.

1. Additional Definitions.

- "**Beta Services**" mean any pre-production version of the Services that are offered by Armor to certain customers for the sole purpose of testing and evaluating such services. The terms and conditions for your participation in any Beta Services is set forth in Attachment 1.
- "**Services Commencement Date**" means the date Armor first provisions the Services to you and the date the Recurring Fees commence.
- "**Support**" means the telephone and online technical support provided in connection with the Services.
- "**Term**" means the Initial Term and any Renewal Term, as defined by the Solutions Order, for the Services.

2. Armor Responsibilities. Armor will begin provisioning the Services and Support once an Order has been executed for the Term in accordance with the MSA and this Schedule. Armor has, and will maintain during the Term, the following certifications:

- HITRUST Certification (to the extent the HITRUST organization continues to offer such certification or until an official HHS/OCR certification becomes available);
- PCI-DSS Level 1 Service Provider;
- SSAE 16 SOC 2 Type II; and
- ISO 27001.

3. Your Responsibilities.

A. You agree to comply with all laws applicable to your use of the Services and the restrictions set forth in the AUP. To the extent you use the Services to provide hosting services to End Users, you must ensure that your End Users comply with the AUP. You agree to immediately notify Armor of any unauthorized use of your account or any other breach of security as it relates to the Services, and to reasonably cooperate with Armor's investigation of service outages or security issues.

B. If you will use the Services to transmit, process, or store payment card information ("cardholder data" as defined in the current version of the Payment Card Industry Data Security Standard ("PCI DSS")), or protected health information ("**PHI**") as defined under the HIPAA/HITECH/Omnibus Rule regulations, you must disclose such intended use to Armor prior to any such transmission and/or storage and execute a Business Associate Agreement (BAA) and/or PCI Addendum to meet our respective obligations under federal regulations.

4. Invoicing/Billing.

A. Your initial invoice will include the pro-rated Recurring Fees and Non-Recurring Fees incurred by you between the Services Commencement Date and the initial invoice's date, if applicable, plus the subsequent month's Recurring Fees. Thereafter, Armor will invoice you monthly in advance for the Recurring Fees (and where applicable for Non- Recurring Fees that are fixed and determinable in advance) and in arrears for any other Non-Recurring Fees.

B. The Recurring Fees set forth in the Order will remain fixed during the Initial Term. Upon commencement of any Renewal Term, the Recurring Fees for the Services will be subject to the fees then in-effect at the date of such renewal.

5. Payments. Payment for Services is due on the invoice date. If payment is not made on the invoice date, you will be required to maintain a balance in your account for the first and last month of Services at the commencement of the Term. You will be liable for all costs and expenses incurred by Armor in collecting past due amounts, including reasonable attorneys' fees.

6. Term; Termination; Termination Assistance.

A. This Schedule and your subscription(s) for the Services will be for the Initial Term and each will automatically renew for successive Renewal Terms for a period equal to the Initial Term at the end of the Initial Term and each Renewal Term; provided, however, that either party may terminate the Services subscription effective at the end of the Initial Term or then-current Renewal Term by providing the other with written notice of non-renewal at least thirty (30) days prior to the commencement of the next Renewal Term. You will not be entitled to any credits or refunds for any prepaid Fees in the event of a non-renewal or other expiration. Both parties will communicate any non-renewal notice through the Armor customer portal.

B. To the extent applicable to your Services, should you at or following termination of the Services desire assistance from Armor in migrating your Services Data stored on the servers provided to you by Armor to an alternative service or vendor, Armor agrees to provide reasonable migration assistance subject to you (i) requesting such assistance in writing prior to or immediately following such termination, (ii) entering into a separate Professional Services Agreement; (iii) agreeing to pay Armor's then standard professional Fees; (iv) and reimburse Armor for any actual and reasonable out of pocket expenses incurred in providing such migration services.

7. Maintenance. Armor may from time to time conduct routine tests, maintenance, upgrade or repair on any part of its networks, infrastructure, or the Services ("**Scheduled Maintenance**"), and will use commercially reasonable efforts to provide prior notice (including at least fourteen (14) days' prior notice for any customer-impacting maintenance). Armor will seek to perform scheduled maintenance outside of business hours (defined as Monday to Friday 09:00 to 18:00 of the time zone of the relevant datacenter). You acknowledge that in some instances it may not be practical for Armor to give advance notice of maintenance, for example, in the event of an unforeseen disruption of Services ("**Emergency Maintenance**"). In these cases, Armor has the right to disrupt Services without prior notice.

8. Data Security. In the ordinary course of the use of the Services, you will maintain access to and administrative domain and control of your Services Data, including any cardholder data, PHI, personally identifiable information ("**PII**") or other Confidential Information that may reside within your Services Data. You acknowledge that as a result of Armor accessing your Services, Armor may also have the ability to view or control your Services Data and in such an event, Armor will maintain your Services Data as Confidential Information and will not make any use of your Services Data other than as requested by you or necessary to perform the Services. Nothing in this Agreement will be deemed to impose any duty or obligation on Armor's behalf to supervise or advise you on the manner in which you administer access to and control of your Services Data. Armor does have access to limited PII (typically name, address, telephone number and email addresses for your contact personnel involved in the receipt of the Services) and similar Confidential Information to the extent included within your Account Data, and Armor agrees to protect such information per the provisions in this Section.

12. Warranty Requirements. Notwithstanding Armor's warranty of Services in the MSA, YOU ARE SOLELY RESPONSIBLE FOR IMPLEMENTING ADEQUATE FIREWALL, PASSWORD AND OTHER SECURITY MEASURES TO PROTECT YOUR SYSTEMS, DATA AND APPLICATIONS FROM UNWANTED INTRUSION, WHETHER OVER THE INTERNET OR BY OTHER MEANS.

13. Limitation of Liability. EXCEPT TO THE EXTENT SET FORTH IN ANY APPLICABLE SERVICE LEVEL AGREEMENT, ARMOR WILL HAVE NO LIABILITY SHOULD THERE BE ANY DELAY IN THE DELIVERY OF THE SERVICES. ARMOR ASSUMES NO RESPONSIBILITY FOR THE BACK UP OR INTEGRITY OF YOUR SERVICES

DATA, AND, EXCEPT FOR ARMOR'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, IN NO EVENT WILL ARMOR BE LIABLE FOR ANY DAMAGES OF ANY KIND RESULTING FROM LOSS OF YOUR SERVICES DATA. This Schedule is subject to the liability limitation provisions in the MSA.

14. Intellectual Property; Hardware and IP Addresses.

A. You may not access or use any aspect of the Services for the purposes of reverse engineering, decompiling, or disassembling the Services or any of their components, or developing a competing product or service, except to the extent that such activity is expressly permitted by applicable law notwithstanding this prohibition. You also agree not to remove, modify or obscure any copyright, trademark or other proprietary rights notices that may be displayed or contained within the Services or any components of the Services.

B. Unless otherwise agreed in writing by the parties, if Armor provides you with any software, hardware, or servers to be used for the provisioning of the Services, you do not acquire any ownership interest in any of the servers, software, or other hardware. Similarly, Armor does not acquire any ownership interest in your Services Data.

C. Some hardware and software components of the Services are provided through or licensed from third parties. Your use of all such components is subject to the terms of this Agreement, as well as the terms and conditions of any applicable end user license or any similar agreements. In some cases, Armor, and not those third parties, will provide Support related to the Services, including support related to those third-party components. Under certain circumstances, pursuant to the terms of applicable third- party license or services agreements, Armor may be obligated to provide certain information to those third parties regarding the Services and/or regarding your identity. You consent to such disclosures.

D. You acknowledge that if you install and host Customer-owned software licenses (each a "License") on Armor's infrastructure or to be used in conjunction with your use of the Services, you warrant and represent that you have and will continue to have the right, license and power under all relevant Licenses and related agreements to which you are a party or subject to have such Licenses installed and hosted on Armor's infrastructure or the Services for your benefit and that you are and will continue to remain in full compliance with such Licenses' terms and conditions. You further warrant and represent that you have satisfied any and all conditions required for you to exercise such right, license and power. In addition, you agree to indemnify, defend and hold Armor and its Affiliates harmless from (i) any and all third party claims, and any related losses, liabilities, fines or expenses (including reasonably attorneys' fees) incurred by Armor, relating to your compliance with such License agreements or your alleged unauthorized use or installation of such Licenses, and (ii) any other costs or expenses incurred by Armor in connection with or as a result of any software audit performed on Armor on the Licenses by the software vendor or any of its authorized resellers or agents, regardless of your compliance with the Licenses.

E. You acknowledge and agree that any IP addresses that Armor may assign to you in connection with the Services are registered to and owned by Armor and upon any expiration or termination of this Agreement, you agree to release and cease using any such IP addresses.

15. API License.

A. To the extent your Services includes a license to the Armor application program interface ("**API**") and any sample code or scripts ("**Sample Code**"), Armor hereby grants to you and your authorized Users, during the Term, a non-exclusive, non-transferable license (without the right to sublicense) to use the API components to (i) develop and implement applications to assist you and your authorized Users to access and use various Services (the "**API Applications**"); and (ii) use, copy and modify any Sample Code provided as part of the API for the sole purposes of designing, developing, and testing your API Applications. You may not generally distribute (commercially or otherwise) your API Applications, without expressed written consent from Armor, but you may make copies of and make the API Applications available to your authorized Users for the purpose of accessing and using the Services. You may not use the API for or in conjunction accessing and using any product or service offerings of third parties that are competitive with the Services.

B. You agree not to remove or destroy any copyright notices, other proprietary markings or confidentiality legends placed upon or contained within the API components. You may not use, copy, modify, display, rent, lease, loan, transfer, distribute, download, merge, make any translation or derivative work or otherwise deal with the API, except as expressly provided in this Agreement. In no event may you cause or permit the disassembly, reverse compilation or other decoding of any portion of the API that is provided in object code only format, or otherwise attempt to obtain, derive or modify the source code or architecture of such portions of the API; provided, however, that the foregoing restriction is not intended to apply to Sample Code specifically provided for the purpose of modification and inclusion in your API Applications. You may not use the API in any manner that would breach this Agreement. Armor may not provide Support for your use of a specific API. Armor may revise or cease to provide the API, Sample Code or its functionality or any part thereof, or support for an API from time to time without notice.

16. General. This Schedule supplements the MSA with respect to the Services subject to the Schedule. If any terms and conditions in a signed Order by their terms expressly vary the terms of this Schedule, such terms and conditions of the Order will prevail. The following Attachments also apply to the Services subject to this Schedule.

ATTACHMENT 1:
BETA SERVICES ADDENDUM

If you elect to participate in any evaluation or test of any Beta Services, then the following conditions will apply.

A. You acknowledge that: (i) such Beta Services are provided "AS IS, AS AVAILABLE" with no warranty whatsoever; (ii) the Beta Services are a pre-release, pre-production version and may not work properly and that your use of the Beta Services may expose you to unusual risks of operational failures; (iii) Beta Services should not be used in a live production environment; and (iv) you must not use the Beta Services where their use could affect any systems relating to the control of hazardous environments, life support, or weapons systems.

B. You agree to provide prompt feedback regarding your experience with the Beta Services in a form reasonably requested by us, including information necessary to enable us to duplicate errors or problems that you may experience. You agree that all information regarding your beta test, including your experience with and opinions regarding the Beta Services, will be deemed our Confidential Information, as defined above, and you agree not to disclose such testing results or experiences with any third party or use them for any purpose other than providing feedback to Armor.

C. You agree that we may use your feedback for any purpose whatsoever, including product development purposes. At our request, you will provide us with comments that we may use publicly for press materials and marketing collateral. Any intellectual property inherent in your feedback or arising from your testing of the Beta Services will be owned exclusively by Armor.

D. The commercially released version of the Beta Services may change substantially from the pre-release version, and programs that use or run with the pre-release version may not work with the commercial release or subsequent releases.

E. You are not entitled to any Service Credits under any Service Level Agreement for downtime or other problems that may result from your use of the Beta Services. Subject to the foregoing limitations, the maximum aggregate liability of Armor and any of its employees, agents, affiliates, or suppliers, under any theory of law (including breach of contract, tort, strict liability, and infringement) for harm to you arising from your use of the Beta Services will be a payment of money not to exceed One Hundred Dollars ($100.00).

F. Armor may terminate the Beta Services at any time without notice, in its sole discretion.

ATTACHMENT 2:
ADDITIONAL OR ADJUSTED TERMS FOR SERVICES PROVIDED IN EMEA and ASIA

For a Customer located in EMEA or Asia, the Services will be provided by Armor Defense Ltd., and references in the MSA and this Schedule to "Armor" will be deemed to refer to Armor Defense Ltd. In addition, the following provisions will apply, and will amend both the MSA and the foregoing Schedule to the extent of any inconsistency or conflict.

1. Additional Definitions.

"**Business Day**" means any day that is not a Saturday, Sunday or a public holiday in the United Kingdom.

"**Data Breach**" means any breach of Armor's obligations under Section 2 below, other loss, destruction, damage of, or compromise to, Personal Data or any other event relating to Services Data which falls within the definition of "personal data breach" set out below).

"**Data Exporter**" has the meaning given in Article 3 of The Model Clauses Decision.

"**Data Importer**" has the meaning given in Article 3 of The Model Clauses Decision.

"**DPA**" means the Data Protection Act 2018 (as amended from time to time).

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) as supplemented and modified by the DPA, and to the extent that the GDPR does not apply to processing of personal data by either of the parties, any applicable GDPR Replacement Legislation.

"**GDPR Replacement Legislation**" means any legislation relating to the processing of personal data effective in the United Kingdom which is intended to replicate or maintain some or all of the provisions, rights and obligations set out in the GDPR in circumstances where the GDPR is no longer applicable in the UK because the United Kingdom is no longer a member of the European Union (and where appropriate, references to "Article" or "Chapter" in this Agreement shall be to the equivalent provision of the GDPR Replacement Legislation).

"**Model Clauses Agreement**" means any contract which (i) is in the form set out in the Annex to The Model Clauses Decision; or (ii) falls within the scope of Article 7(2) of The Model Clauses Decision.

"**The Model Clauses Decision**" means the Commission Decision 2010/87/EU.

"**Privacy Laws**" means the DPA, GDPR, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all Applicable Laws relating to the processing of Personal Data and privacy (including any legislation amending or replacing the same).

"**Privacy Shield**" means the E.U. - U.S. Privacy Shield administered by the U.S. Department of Commerce which was subject to a finding of adequacy by the European Commission pursuant to Article 25(6) of Directive 95/46/EC, as recorded in Decision 2016/1250 dated 12 July 2016.

"**Services Data**" means the data, which may include Personal Data in respect of which Customer is data controller (as defined in the GDPR), or other information transmitted to or from, stored on or otherwise processed by the Infrastructure Platform or servers provided to you by Armor, whether hosted by you, Armor, or a third-party provider, in connection with the provision of the Services. For clarification, Account Data is excluded from this definition.

"**Statutory Processor Obligations**" means the contractual obligations which a data controller is required to impose on a data processor under Article 28(3), if and to the extent that they are not imposed on Armor under this Agreement.

2. Data Protection.

A. All terms used in this Clause 2 which are not otherwise defined above or in the Agreement will have the meaning ascribed to them in the GDPR unless otherwise stated or self-evident from the context.

B. As between the parties, all Personal Data processed under or in connection with this Agreement will be and will remain the property of Customer.

C. Armor acknowledges that in respect of any processing of Personal Data by Armor under or in connection with this Agreement, Armor shall be acting as data processor and Customer shall be acting as data controller.

D. The parties warrant and represent that in relation to this Agreement, each will comply with all the requirements of the Privacy Laws (as may be amended from time to time) and any regulations made under them.

E. The parties agree and acknowledge that this Section 2 is intended to ensure compliance with Article 28(3) of the GDPR and accordingly the parties have documented the subject-matter, duration, nature and purpose of the processing, the type of personal data and categories of data subject as set out in subschedule 4-A of this Attachment. The obligations and rights of Customer, as data controller, are set out in this Section 2.

F. The parties agree that the Statutory Processor Obligations shall be fully incorporated into this Agreement and in the event of any conflict between the Statutory Processor Obligations and any other provision of this Agreement, the Statutory Processing Obligations shall prevail and apply. Armor shall comply with the Statutory Processing Obligations.

G. To the extent that Armor processes Services Data that includes Personal Data, it shall:

1. only use the Personal Data for the legitimate purposes of performing its obligations under this Agreement and for no other purposes unless instructed to do so by Customer;
2. process the Personal Data only on documented instructions from Customer given from time to time, in writing, save to the extent that Armor is required to do otherwise by Union or Member State law ("Legal Requirement") to which Armor is subject; in such a case, Armor shall inform Customer of that Legal Requirement before processing, unless that law prohibits it from providing such information on important grounds of public interest;
3. inform Customer if, in its opinion, any instruction from Customer relating to the processing of Personal Data infringes the GDPR or any Privacy Laws;
4. immediately notify Customer if it is contacted or approached in relation to: (i) any data subject seeking to exercise his/her rights set out in Chapter III, including but not limited to any subject access request under the GDPR; (ii) any other request from a data subject; (iii) any claim for damages under the Privacy Laws; and/or (iv) any investigation or enforcement activity by the Information Commissioner or any other regulator, in each case relating to, connected with, or arising out of, Armor's processing of

Personal Data; provided, in each case, Armor shall not be liable in cases where Customer fails to respond to the Data Subject's request in total, correctly or in a timely manner;

5. taking into account the nature of the processing, assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer obligation to respond to requests for exercising the data subject's rights laid down in Chapter III, in respect of Services Data;

6. to the extent Armor reasonably has access to the relevant data subject's Personal Data, and without prejudice to its other obligations in this Clause 2, provide to Customer all reasonable assistance and cooperation Customer requests in relation to any request, claim, investigation or enforcement activity notified to Customer pursuant to Section G4 above, any claim and/or exercise or purported exercise of rights by a data subject under Privacy Laws or any investigation or enforcement activity by the Information Commissioner or any other regulator, relating to, connected with or arising out of Armor's processing of Personal Data;

7. not engage another processor to process Personal Data (or otherwise sub-contract or outsource the processing of any of the Personal Data to any third party, except the affiliates or authorized subcontractors as stated in subschedule 4A to this Attachment unless it has complied with Articles 28(2) and 28(4) and obtained the prior written consent of Customer. In its absolute discretion, Customer may provide consent to Armor's use of a third-party processor (not to be unreasonably delayed). Consent granted shall be conditional on Armor obtaining the third party's written agreement to abide by and honor terms relating to the processing of Personal Data which are the same as those imposed on Armor under this Agreement. If Customer objects to Armor's use of such a third-party subcontractor, Customer shall notify Armor in writing within five (5) Business Days after the receipt of Armor's written request to appoint a third-party subcontractor. In the event that Customer objects to a third-party subcontractor, it shall provide its material or legal reasons for such objections;

8. take all measures required pursuant to Article 32 and ensure that appropriate technical and organizational measures are in place, to ensure the security of Personal Data and that appropriate technical and organizational measures are taken against unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data.

9. take reasonable steps to ensure the reliability of any of its personnel who have access to Personal Data and ensure that personnel authorized to process Personal Data are subject to appropriate obligations of confidentiality pursuant to Article 28(3)(b);

10. assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to Armor;

11. not transmit or transfer any Personal Data to any country or place outside the European Economic Area (save for any transfer to the United Kingdom in circumstances where the United Kingdom is not part of the European Economic Area) ("**Transferred Data**") unless: (i) the parties procure that (a) the Data Exporter and Data Importer in respect of any such Transferred Data are party to, and comply with, a Model Clauses Agreement at all material times and (b) the Model Clauses Agreement remains in place until Armor and any of its sub- processors ceases to process any Transferred Data; or (ii) the transfer is to Armor, or a sub-contractor of Armor, which is and shall for the term of this Agreement remain certified under the Privacy Shield or have entered into a Model Clauses Agreement to effectuate the processing of the Transferred Data, and Armor shall (and shall require that any relevant sub-contractor shall) in relation to any processing of Transferred Data comply fully with all obligations arising out of the Privacy Shield including the Privacy Shield Framework Principles or the Model Clauses Agreement, and shall notify Customer immediately if at any time it fails to be certified under the Privacy Shield or fully compliant with it or the Model Clauses Agreement;

12. make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow Customer and/or its representatives access to premises (including all locations where Armor may process Personal Data) during normal business hours to audit and inspect the processing and storage of Personal Data being performed under or in connection with this Agreement. Armor shall also, at Customer's cost (unless such audit or inspection is carried out in connection with, or demonstrates, a breach of this Section 2, in which case this shall be at Armor's cost), provide to Customer and/or its representatives all reasonable assistance in the performance of such an audit or inspection. For the avoidance of doubt, such audit shall only relate to the Infrastructure Platform provided by Armor to process Customer Personal Data. Armor shall not be obligated to disclose any

information related to other servers and/or information used to process personal information related to its other customers;

13. inform Customer immediately on becoming aware of a Data Breach and co-operate fully with Customer in respect of the measures that should be taken in response. Armor shall also co-operate fully with Customer in respect of any matter which in the opinion of Customer is required for ensuring Customer' continued compliance with the Privacy Laws. For the avoidance of doubt, the cooperation of Armor under this Section 12 shall be provided solely at Armor's own cost and will include, without limitation, providing Customer and/or its representatives access to any premises under Armor's control (if necessary without notice); and

14. at the end of provision of services relating to processing Personal Data, or upon receipt of a written request from Customer if earlier, Armor will destroy such of the Personal Data as is in its possession in such a way as to render the Personal Data irrecoverable by any means (save to the extent that applicable Union or Member state law requires it to retain any Personal Data), after having returned or provided all Personal Data to Customer or its representatives if so requested by Customer.

3. Limitation of Liability Adjustments. The parties respective liability:

(A) for gross negligence or willful misconduct related to this Agreement or the Services;
(B) for death or personal injury caused by its negligence or the negligence of its employees or agents;
(C) for fraud or fraudulent misrepresentation;
(D) under any of the express indemnities contained in this Agreement;
(E) to pay sums properly due and owing to the other in the course of normal performance of this Agreement; or
(F) any other matter which cannot by law be excluded;

IS NOT EXCLUDED OR LIMITED BY THIS AGREEMENT, EVEN IF ANY OTHER TERM OF THIS AGREEMENT WOULD OTHERWISE SUGGEST THAT THIS MIGHT BE THE CASE.

4. Notices. Except to the extent that notices may be sent by electronic mail or via the Armor customer portal as specifically set forth in this Agreement, notices sent to Armor under this Agreement will be sent to Armor Defense Ltd., 268 Bath Road, Slough, Berkshire SL14AX, Attn: Legal.

5. Third Party Rights: No term of this Agreement will be enforceable under the Contracts (Rights of Third Parties) Act 1999 by a person who is not a party to this Agreement.

6. Governing Law; Jurisdiction. The Agreement will be governed by the laws of England and Wales and you hereby submit to the exclusive jurisdiction of the courts of England and Wales. The United Nations Convention on Contracts for the International Sale of Goods (1980) will not apply. This Section over-rides the arbitration provision contained in the MSA.

SUBSCHEDULE 2A
ARTICLE 28 DATA PROCESSING INFORMATION

The purpose of this Schedule 4A is to ensure the parties comply with their obligations as set out in the part of Article 28(3) of the GDPR which states that:

"Processing by a processor shall be governed by a contract … that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller."

Clause 2 of this Schedule and/or other provisions of this Agreement set out most of the information detailed above, including the obligations and rights of the data controller. For completeness we set out further information below.

Subject matter

- The processing of Personal Data by Armor shall be undertaken in the context of the provision of the Services under this Agreement.

Duration

- Armor shall process Personal Data during the Term of this Agreement, unless this Agreement is terminated earlier.

Nature and purpose of processing

- Armor shall process Personal Data for the purpose of providing the Services.

Type of personal data

- It is envisaged Armor shall process names and work email addresses of Customer's employees, suppliers and partners.

Categories of data subjects

- Armor shall process Personal Data of Customer's employees, suppliers and partners.

Obligations and rights of the data controller

- The obligations and rights of the data controller are set out in Clause 2 of this Schedule.

SUBSCHEDULE 4B
SUBCONTRACTORS WHO PROCESS CUSTOMER PERSONAL DATA ON BEHALF OF ARMOR

Description of the subcontractors used by Armor and the purposes for which the subcontractor's services are utilized in accordance with Clause 2 of this Schedule:

Subcontractor	Purpose	Personal Data Processed	Applicable Services
JIRA	Armor Management Portal (AMP) ticketing system	User name; email address	Armor Enterprise for Cloud Armor Agent for Servers
AuthSMTP.com	Customer communication tool for Email	Email address	Armor Enterprise for Cloud Armor Agent for Servers
Coalfire	Vulnerability scanning tool	User name; email address; work address	Armor Enterprise for Cloud
Full Story	User session recorder to provide troubleshooting and/or product feedback	User name; email address; phone	Armor Enterprise for Cloud Armor Agent for Servers
Global Sign	SSL certificates	User name; email address; work address	Armor Enterprise for Cloud
Marketo	Marketing database and automation	User name; email address; work address; telephone number	Armor Internal Corporate IT Systems

Subcontractor	Purpose	Personal Data Processed	Applicable Services
Bizible	Marketing channel attribution	User name; email address; telephone number;	Armor Internal Corporate IT Systems
Klientboost	Pay Per Click Search	User name; email address; work address; telephone number	Armor Internal Corporate IT Systems
Strongpages	Search Engine Optimization	User name; email address; work address; telephone number	Armor Internal Corporate IT Systems
Etumos	Email verification service	Email address	Armor Internal Corporate IT Systems
SalesForce	Sales database	User name; email address; work address; telephone number	Armor Internal Corporate IT Systems
SalesLoft	Customer communication tool for Email	User name; email address; work address; telephone number	Armor Internal Corporate IT Systems

SUBSCHEDULE 2C
ARMOR'S TECHNICAL AND ORGANIZATIONAL
SECURITY MEASURES FOR THE PROCESSING OF PERSONAL DATA

This subschedule is without prejudice to Armor’s obligations set out in Clause 2 of this Schedule.

Data Processor will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Armor secure customer portal and stored on other Armor controlled systems including the secure virtual servers provided by Armor for Customer to store Personal Data.

Armor maintains an information security program that has been certified against the ISO/IEC 27001:2013 standard. The program includes an information security policy, and other corporate policies and procedures that are designed to give Armor the capability to protect non-public personal information consistent with applicable federal, state, and international regulations. In addition to ISO 27001 certification, Armor also holds unqualified SSAE 16 SOC 2 Type II reports that further validate Armor’s information security program.

Users of confidential and private information within Armor aim to keep the volume of such material to a reasonable level in proportion to the business responsibilities and services being delivered to customers, employees, and other parties.

Personnel security measures include employees undergoing a multi-component background check as part of the hiring process in accordance with applicable law. Employees are required to sign confidentiality and non-disclosure agreements as a condition of employment.

Vendor management procedures are in place to review contractors, business partners, and vendors that will have access to confidential information.

Armor’s secure cloud hosting environments including all of the services Armor provides to customers have been validated against the Payment Card Industry Data Security Standard v3.2 and the HITRUST CSF. These validations require controls designed to help protect the confidentiality and integrity of Customer’s Personal Data. These controls include the following:

- IP Reputation Management
- DoS/DDoS mitigation
- Web Application Firewalls
- Network Intrusion Detection (NIDS)
- Hypervisor based network firewall resident on each Customer virtual server
- Managed anti-malware/anti-virus protection
- Operating system file integrity monitoring
- Operating system patching
- Operating system log management

`

Armor provides for only secure, encrypted remote access by Customer for administrative access to its servers and controls Armor support staff access to Customer servers for support purposes via secure, two factor authenticated jump servers and a privileged access management system that logs and fully records each Armor session.

Data Processor will not materially decrease the overall security of the Armor Services during the Term.