HackerOne Inc.

Carahsoft Rider to Product Specific License Terms and Conditions (for U.S. Government End Users)

1. **Scope**. This Rider and the attached HackerOne Inc. ("Manufacturer") product specific license terms establish the terms and conditions enabling Carahsoft ("Contractor") to provide Manufacturer's information technology products and services to Ordering Activities under Carahsoft's GSA MAS contract number 47QSWA18D008F (the "Schedule Contract"). Installation and use of the information technology shall be in accordance with this Rider and Manufacturer Specific Terms attached hereto, unless an Ordering Activity determines that it requires different terms of use and Manufacturer agrees in writing to such terms in a valid delivery order placed pursuant to the Schedule Contract.

2. **Applicability**. Whereas GSA and Carahsoft agreed at the time of Schedule Contract award upon a base set of terms and conditions applicable to all manufacturers and items represented on the Schedule Contract; and Whereas, the parties further agreed that all product specific license, warranty and software maintenance terms and conditions would be submitted at the time each new manufacturer was to be added to the Schedule Contract; Now, Therefore, the parties hereby agree that the product specific license, warranty and software maintenance terms set forth in Attachment A hereto (the "Manufacturer Specific Terms" or the "Attachment A Terms") are incorporated into the Schedule Contract, but only to the extent that they are consistent with Federal law (*e.g.*, the Anti-Deficiency Act (31 U.S.C. § 1341), the Contracts Disputes Act of 1978 (41 U.S.C. §§ 7101 *et seq*.), the Prompt Payment Act (31 U.S.C. §§ 3901 *et. seq*.), the Anti-Assignment statutes (31 U.S.C. § 3727 and 41 U.S.C. § 15), DOJ's jurisdictional statute 28 U.S.C. § 516 (Conduct of Litigation Reserved to the Department of Justice (DOJ), and 28 U.S.C. § 1498 (Patent and copyright cases)). To the extent any Attachment A Terms are inconsistent with Federal law (See, FAR 12.212(a)), such inconsistent terms shall be superseded, unenforceable and of no legal force or effect in all resultant orders under the Schedule Contract, including but not limited to the following provisions:

a) **Contracting Parties.** The GSA Customer ("Licensee") is the "Ordering Activity", defined as the entity authorized to order under GSA MAS contracts as set forth in GSA Order OGP 4800.2I, as may be revised from time to time.

b) **Changes to Work and Delays.** Subject to GSAR Clause 552.238-81, Modifications (Federal Supply Schedule) (April 2014) (Alternate I – JUN 2016) and (Alternate II – JUN 2016), and 52.212-4(f) Excusable Delays (JUN 2010) regarding which the GSAR and the FAR provisions take precedence.

c) **Contract Formation.** Subject to FAR 1.601(a) and FAR 43.102, the GSA Customer Purchase Order must be signed by a duly warranted Contracting Officer, in writing. The same requirement applies to contract modifications affecting the rights of the parties. All terms and conditions intended to bind the Government must be included within the contract signed by the Government.

d) **Termination**. Clauses in the Manufacturer Specific Terms referencing termination or cancellation are superseded and not applicable to any GSA Customer order. Termination shall be governed by the FAR, the underlying GSA Schedule Contract and the terms in any applicable GSA Customer Purchase Orders. If the Contractor believes the GSA Customer to be in breach, it must file a claim with the Contracting Officer and continue to diligently pursue performance. In commercial item contracting under FAR 12.302(b), the FAR provisions dealing with disputes and continued performance cannot be changed by the Contracting Officer.

e) **Choice of Law.** Subject to the Contracts Disputes Act, the validity, interpretation and enforcement of this Rider shall be governed by and construed in accordance with the Federal laws of the United States. In the event the Uniform Computer Information Transactions Act (UCITA) or any similar Federal laws or regulations are enacted, to the extent allowed by Federal law, they will not apply to this Rider or the underlying Schedule Contract.

f) **Equitable remedies**. Equitable remedies are generally not awarded against the Government absent a statute providing therefore. In the absence of a direct citation to such a statute, all clauses in the Manufacturer Specific Terms referencing equitable remedies are superseded and not applicable to any GSA Customer order.

g) **Unilateral Termination.** Unilateral termination by the Contractor does not apply to a GSA Customer Purchase Order and all clauses in the Manufacturer Specific Terms referencing unilateral termination rights of the Manufacturer are hereby superseded.

h) **Unreasonable Delay.** Subject to FAR 52.212-4(f) Excusable delays, the Contractor shall be liable for default unless the nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and without its fault or negligence such as, acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. The Contractor shall notify the Contracting Officer in writing as soon as it is reasonably possible after commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch and shall promptly give written notice to the Contracting Officer of the cessation of such occurrence.

i) **Assignment.** All clauses regarding the Contractor's assignment are subject to FAR 52.232-23, Assignment of Claims (JAN 1986) and FAR 42.12 Novation and Change-of-Name Agreements (Sep. 2013). All clauses governing the Contractor's assignment in the Manufacturer Specific Terms are hereby superseded.

j) **Waiver of Jury Trial.** Waivers of Jury Trials are subject to FAR 52.233-1 Disputes (JULY 2002). The Government will not agree to waive any right that it may have under Federal law. All clauses governing a waiver of jury trial in the Manufacturer Specific Terms are hereby superseded.

k) **Government Indemnities.** This is an obligation in advance of an appropriation that violates anti-deficiency laws (31 U.S.C. § 1341 and 41 U.S.C. § 6301), since the GSA Customer commits to pay an unknown amount at an unknown future time. The violation occurs when the commitment is made, i.e., when the agreement featuring this clause is incorporated into a Government contract, and not when the clause is triggered. The Interim FAR Rule dated June 21, 2013 and the Office of Legal Counsel opinion dated March 12, 2012 prohibit such indemnifications. All Manufacturer Specific Terms referencing customer indemnities are hereby superseded.

l) **Contractor Indemnities.** All Manufacturer Specific Terms that violate DOJ's jurisdictional statute (28 U.S.C. § 516) by requiring that the Government give sole control over the litigation and/or settlement to the Contractor are hereby superseded. Nothing contained in the Manufacturer's Specific terms shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute.

m) **Renewals.** All Manufacturer Specific Terms that provide for automatic renewals violate the Anti-Deficiency Act and are hereby superseded. This is an obligation in advance of an appropriation that violates anti-deficiency laws (31 U.S.C. § 1341 and 41 U.S.C. § 6301), since the GSA Customer commits to pay an unknown amount at an unknown future time. The violation occurs when the commitment is made, i.e., when the agreement featuring this clause is incorporated into a Government contract, and not when the clause is triggered.

n) **Future Fees or Penalties.** All Manufacturer Specific Terms that require the Government to pay any future fees, charges or penalties are hereby superseded unless specifically authorized by existing statutes, such as the Prompt Payment Act (31 U.S.C. § 3901 et seq.) or Equal Access To Justice Act (5 U.S.C. § 504; 28 U.S.C. § 2412).

o) **Taxes.** Taxes are subject to FAR 52.212-4(k), which provides that the contract price includes all applicable federal, state, local taxes and duties. Contractor shall state separately on its invoices, taxes excluded from the fees, and the GSA Customer agrees to either pay the amount of the taxes (based on the current value of the equipment or services) to Contractor or provide it evidence necessary to sustain an exemption, in accordance with FAR 52.229-1 and FAR 52.229-3.

p) **Third Party Terms.** When the end user is an instrumentality of the U.S., no license terms bind the GSA Customer unless included in the EULA, and the EULA is made an attachment to the underlying GSA Schedule Contract. All terms and conditions affecting the GSA Customer must be contained in a writing signed by a duly warranted Contracting Officer. Any third party manufacturer shall be brought into the negotiation, or the components acquired separately under federally-compatible agreements, if any.

q) **Dispute Resolution and Standing.** Any disputes relating to the Manufacturer Specific Terms or to this Rider shall be resolved in accordance with the FAR, the underlying GSA Schedule Contract, any applicable GSA Customer Purchase Orders, and the Contract Disputes Act. The Ordering Activity expressly acknowledges that Carahsoft as contractor, on behalf of the Manufacturer, shall have standing to bring such claim under the Contract Disputes Act.

r) **Advertisements and Endorsements.** Pursuant to GSAR 552.203-71, use of the name or logo of any U.S. Government entity is prohibited. All Manufacturer Specific Terms that allow the Contractor to use the name or logo of a Government entity are hereby superseded.

s) **Public Access to Information.** Carahsoft agrees that the attached Manufacturer Specific Terms and this Rider contain no confidential or proprietary information and acknowledges the Rider shall be available to the public.

t) **Confidentiality.** Any provisions in the attached Manufacturer Specific Terms that require the Ordering Activity to keep certain information confidential are subject to the Freedom of Information Act (5 U.S.C. § 552), and any order by a United States Federal Court. When the end user is an instrumentality of the U.S. Government, neither this Rider, the Manufacturer's Specific Terms nor the Schedule Price List shall be deemed "confidential information" notwithstanding marking to that effect. Notwithstanding anything in this Rider, the Manufacturer's Specific Terms or the Schedule Contract to the contrary, the GSA Customer may retain such Confidential Information as required by law, regulation or its bonafide document retention procedures for legal, regulatory or compliance purposes; provided however, that such retained Confidential Information will continue to be subject to the confidentiality obligations of this Rider, the Manufacturer's Specific Terms and the Schedule Contract**.**

u) **Alternate Dispute Resolution**. The GSA Customer cannot be forced to mediate or arbitrate. Arbitration requires prior guidance by the head of a Federal agency promulgated via administrative rulemaking according to 5 U.S.C. § 575(c). GSA has not issued any because it considers the

Board of Contract Appeals to be an adequate, binding ADR alternative. All Manufacturer Specific Terms that allow the Contractor to choose arbitration, mediation or other forms of alternate dispute resolution are hereby superseded.

v) **Ownership of Derivative Works**. Provisions purporting to vest exclusive ownership of all derivative works in the licensor of the standard software on which such works may be based are superseded. Ownership of derivative works should be as set forth in the copyright statute, 17 U.S.C. § 103 and the FAR clause at 52.227-14, but at a minimum, the GSA Customer shall receive unlimited rights to use such derivative works at no further cost.

3. Order of Precedence/Conflict. To the extent there is a conflict between the terms of this Rider and the terms of the underlying Schedule Contract or a conflict between the terms of this Rider and the terms of an applicable GSA Customer Purchase Order, the terms of the GSA Schedule Contract or any specific, negotiated terms on the GSA Customer Purchase Order shall control over the terms of this Rider. Any capitalized terms used herein but not defined, shall have the meaning assigned to them in the underlying Schedule Contract.

ATTACHMENT A

HACKERONE INC.

MANUFACTUER SPECIFIC TERMS (FOR U.S. GOVERNMENT END USERS)

These HackerOne Inc. ("HackerOne") Manufacturer Specific Terms (these "***Terms***") govern the use of HackerOne's software as a service Solutions (the "Services") by customers ("Customers" or "Ordering Activities") purchasing the Services under Carahsoft's GSA MSA contract number GS-35F-0511T.

1. DEFINITIONS. The following capitalized terms used herein shall have the meanings given to them below:

A. "**Affiliate**" means any entity which controls, is controlled by or under common control with a party, where "control" means ownership or control, direct or indirect, of fifty percent (50%) or more of such entity's voting capital, and any such entity shall be an affiliate of such party only as long as such ownership or control exists.

B. **"Applicable Law"** shall mean all laws (including the requirements of any government or regulatory authority) applicable to a party and/or the Services under these Terms for the time being in force in the relevant jurisdiction. These include but are not limited to anti-money laundering, anti-bribery, data privacy, export and intellectual property laws.

C. "**Confidential Information**" means any confidential or proprietary business or technical information about a party disclosed by it or its Affiliates or made available in connection with these Terms, whether disclosed in written, oral, electronic or visual form, which is identified as confidential at the time of disclosure or should reasonably be understood to be confidential given the nature of the information and the circumstances surrounding the disclosure, including without limitation business, operations, finances, technologies, products and services, pricing, personnel, customer and suppliers, including the HackerOne Platform and the content of Finder Submissions. Confidential Information does not include any information that (i) was publicly known and made generally available in the public domain prior to the time of disclosure by the disclosing party; (ii) becomes publicly known and made generally available after disclosure by the disclosing party to the receiving party; (iii) is already in the possession the receiving party at the time of disclosure by the disclosing party; (iv) is obtained by the receiving party from a third party without a breach of such third party's obligations of confidentiality; or (v) is independently developed by the receiving party without use of the disclosing party's Confidential Information.

D. **"Customer Report"** means a report or similar documentation made available by HackerOne to Customer through the HackerOne Platform or otherwise that summarizes or is based upon Finder Submissions, including, without limitation, penetration test reports, checklist reports, re-testing reports and similar documentation regarding Finder activities related to a Program.

E. "**Feedback**" means any feedback, comments or suggestions for improvements to the Services.

F. "**Finder**" means an individual or entity using the HackerOne Platform to provide Finder Submissions.

G. **"Finder Submission"** means documents and related materials evidencing a Finder's activities related to a Program, including, without limitation, Vulnerability Reports.

H. "**Finder Terms and Conditions**" means the terms and conditions applicable to Finders at https://www.hackerone.com/terms/finder.

I. "**HackerOne Aggregate Data**" shall have the meaning set forth in Section 6(A) of these Terms.

J. "**HackerOne Fees**" shall have the meaning set forth in Section 4(A) of these Terms.

K. "**HackerOne Platform**" means the software-as-a-service platform offered by HackerOne.

L. "**HackerOne Property**" means any property of any kind, tangible or intangible, which is acquired, created, developed or licensed by HackerOne prior to or outside the scope of these Terms and any improvement or modification thereof and all intellectual property rights therein, including without limitation the HackerOne Platform and Services.

M. "**HackerOne Site**" means HackerOne or its Affiliate's website located at hackerone.com and related domains and subdomains.

N. "**Program**" means the security initiative(s) for which Customer desires to receive Finder Submissions from Finders, which Customer posts to the HackerOne Platform.

O. "**Program Materials**" means the Program Policy, the description of the Program and any other materials made available by Customer to Finders in connection with a Program.

P. "**Program Policy**" means a Customer created description of the security-related and other services that Customer is seeking from Finders, which includes, among other things, the terms, conditions and requirements governing the Program to which the Finders must agree, and the Rewards (if applicable) that Customer may award to Finders who participate in the Program.

Q. **"Reward(s)"** means bounties, grants, pay for effort payments and other financial or non-financial rewards that are awarded to Finders participating in a Program.

R. "**Services**" means HackerOne's software as a service solution made available by HackerOne to Customer through the HackerOne Platform together with any ancillary services purchased by Customer and as set forth in an Order Form. A general description of HackerOne's SaaS solution and examples of such ancillary and related Services provided by HackerOne's program operations and customer success teams or other HackerOne personnel or consultants is set forth in Exhibit A hereto.

S. "**Vulnerability Reports**" means bug reports or other vulnerability information, in text, graphics, image, software, works of authorship of any kind, and information or other material that Finders provide or otherwise make available through the HackerOne Platform to Customer resulting from participation in a Program.

2. HACKERONE PLATFORM AND SERVICES.

A. HackerOne Platform. Customer may access and use the HackerOne Platform solely for its own business purposes in order to connect with Finders and utilize the Services set forth in an Order Form. Among other things, Customer may create Programs and offer Rewards

to Finders for Finder Submissions to such Programs. Finders can browse the Programs and contact Customer through the HackerOne Platform if Finders are interested in participating in such Programs and submitting Finder Submissions for the Programs on the terms described in Finder Terms and Conditions and/or the Program Policy. HackerOne may change all or any part of the HackerOne Platform or HackerOne Site provided that such change in compliance with the terms of these Terms and does not diminish the Services provided to Customer. Customer can submit Feedback regarding the HackerOne Platform and Services by emailing HackerOne at feedback@hackerone.com. By submitting any Feedback, Customer grants to HackerOne a worldwide, perpetual, irrevocable, non-exclusive, transferable, sublicensable, fully-paid and royalty-free license to use, copy, modify, create derivative works based upon and otherwise exploit the Feedback for any purpose. HackerOne acknowledges that the ability to use this Agreement and any Feedback provided as a result of this Agreement in advertising is limited by GSAR 552.203-71.

B. **HackerOne Services.** HackerOne will provide the Services purchased by Customer. The Services may contain links to third-party websites or resources. HackerOne provides these links only as a convenience and is not responsible for the content, products or services on or available from those websites or resources or links displayed on such websites. Customer acknowledges sole responsibility for and assumes all risk arising from Customer's use of any third-party websites or resources. HackerOne may delegate certain rights and obligations relating to the performance of these Terms to its Affiliates, provided however, HackerOne shall be the sole responsible party for all obligations under these Terms and shall ensure the compliance of its Affiliates with these Terms.

C. **Service Level Agreement.** The HackerOne Service Level Agreement, a copy of which is attached as Exhibit B, will apply to HackerOne's provision of the HackerOne Platform and the Services.

3. FINDER SUBMISSIONS AND FINDERS.

A. Unless otherwise expressly agreed to in writing by HackerOne, any use of or reliance on Finder Submissions that Customer receives is at Customer's own risk. HackerOne does not endorse, represent or guarantee the completeness, truthfulness, accuracy, or reliability of any Finder Submission and HackerOne will not be liable for any errors or omissions in any Finder Submission, or any loss or damage of any kind incurred as a result of the use of any Finder Submission.

B. Unless otherwise expressly agreed to in writing by HackerOne, HackerOne does not endorse any Finders, or assume any liability for any damage or harm resulting from Customer's communications or interactions with Finders or other HackerOne customers, either through the HackerOne Platform and Services or otherwise. Any reputation ranking or description of any Finder as part of the Services is not intended by HackerOne as an endorsement of any type. Any selection or use of any Finder is at Customer's own risk.

C. Finders are not employees, contractors or agents of HackerOne, but are independent third parties who want to participate in Programs and connect with Customer through the Services. Unless otherwise expressly agreed to in writing by HackerOne, Customer agrees that any legal remedy that Customer seeks to obtain for actions or omissions of a Finder regarding Customer's Program or Finder Submissions will be limited to a claim against the particular Finder. Any contract or other interaction between Customer and a Finder, including with respect to any Customer Program Policy, will be between Customer and the Finder. HackerOne is not a party to such contracts and disclaims all liability arising from or related to such contracts.

4. FEES.

A. **Fees.** Customer agrees to pay the GSA Schedule Contract holder on behalf of HackerOne all fees for HackerOne's Services (collectively, "**HackerOne Fees**") and any Reward prepayments listed in any applicable Order Form in accordance with the GSA Schedule Pricelist within thirty (30) days of receipt of HackerOne's invoice unless otherwise stated on Order Form. HackerOne, or the GSA Schedule Contract Holder as applicable, will refund any unused Reward prepayments at the end of the term. Except for any amounts disputed in good faith, all undisputed past due amounts will incur interest at a rate indicated by the Prompt Payment Act (31 USC 3901 et seq) and Treasury regulations at 5 CFR 1315.

B. **Taxes.** HackerOne shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with FAR 52.229-1 and FAR 52.229-3.

5. PROGRAMS AND PROGRAM MATERIALS.

A. HackerOne makes available through the HackerOne Platform both managed Programs, under which HackerOne is responsible for the management and the administration of Customer's Programs with input and approval from Customer as mutually agreed throughout the Program, and Programs that are self-managed by Customers. If an Order Form does not specifically identify HackerOne as being responsible for the management and administration of Customer's Programs, then Customer is solely responsible for the management and administration of Customer's Programs through the Services. HackerOne's Vulnerability Guidelines, the current version of which is attached hereto as Exhibit C and is available at https://www.hackerone.com/disclosure-guidelines, describes the default disclosure policy governing vulnerability reporting through the Services and will be applicable to the Services except to the extent Customer adopts its own Program Policy with respect to its Program. In the event of any conflict between Customer's Program Policy and HackerOne's Vulnerability Guidelines, Customer's Program Policy shall prevail.

B. Where any Program is inactive or unattended by Customer, HackerOne shall have the right to remove or disable access to the relevant Program Material and/or pause Finder Submissions if Customer has not responded to HackerOne's written notice (by email) requiring attention within ten (10) business days of such written notice.

C. While HackerOne may assist Customer in preparing Customer's Program Material, Customer is solely responsible for Customer's Program Material.

6. INTELLECTUAL PROPERTY OWNERSHIP AND LICENSES.

A. HackerOne does not claim any ownership rights in any Program Material or Finder Submissions, and nothing in these Terms or otherwise will be deemed to restrict any rights that Customer may have to use and exploit Customer's Program Material and Finder Submissions. Customer acknowledges and agrees that HackerOne may collect aggregated and anonymized statistical and other information from Finder Submissions and Customer's use of the HackerOne Platform and Services ("**HackerOne Aggregate Data**"), which information will not identify particular customers, and may use such information for, among other things, reporting, research, improvements of the Platform and the Services, industry collaboration, and other reasonable business purposes. HackerOne and its licensors exclusively own all right, title and interest in and to the HackerOne Property.

B. By making any Program Material available through the Services, Customer hereby grants to HackerOne a non-exclusive, non-transferable, non-sublicensable, worldwide, royalty-free license to use, copy, reproduce, display, modify, adapt, transmit and distribute copies of Customer's Program Material for the sole purpose of providing the Services.

C. HackerOne hereby grants to Customer a non-exclusive, non-transferable, non-sublicensable, worldwide, royalty-free license to access and view the content and other HackerOne Property that HackerOne makes available on the Services solely in connection with Customer's permitted use of the HackerOne Platform and Services.

D. HackerOne hereby grants to Customer a non-exclusive, non-transferable, non-sublicensable, worldwide, royalty-free license to access and view the Finder Submissions that are made available through the HackerOne Platform and the Services solely in connection with Customer's permitted use of the HackerOne Platform and Services.

E. Subject to HackerOne's ownership of any HackerOne Property contained therein, Customer will own all right, title and interest to each Customer Report. HackerOne hereby grants Customer a non-exclusive, non-transferable, perpetual, worldwide license to access, use and reproduce any HackerOne Property included in each Customer Report.

7. CONFIDENTIALITY; PRIVACY; SECURITY. HackerOne understands that it may receive Confidential Information of Customer, and Customer understands that it may receive Confidential Information of HackerOne. Except as expressly provided in these Terms, the receiving party agrees not to divulge to any third person any Confidential Information of the disclosing party and not to use any Confidential Information of the disclosing party for any purpose not contemplated by these Terms, provided the parties acknowledge and agree that the anonymized HackerOne Aggregate Data is not Confidential Information. HackerOne's Privacy Policy, the current version of which is attached hereto as Exhibit D and which is available at https://www.hackerone.com/privacy, describes how HackerOne collects, uses and discloses information from HackerOne's Customers and Finders and is applicable to the Services. HackerOne will provide the Services and the HackerOne Platform in accordance with HackerOne's Data and Information Security Terms, the current version of which is attached as Exhibit E and is located at https://www.hackerone.com/terms/security. At Customer's request, HackerOne will, on an annual basis, furnish to Customer the current version of any independent third-party attestation report related to the HackerOne Services and Platform.

8. WARRANTY; WARRANTY DISCLAIMER. HackerOne represents and warrants that the HackerOne Platform and the Services provided to Customer will be provided as described in the applicable Order Form, by qualified personnel in a professional manner, and will comply in all material respects with the documentation and content made available by HackerOne with respect thereto. In order to state a claim for breach of the foregoing warranty, Customer must provide notice of such non-compliance within the thirty (30) day period following such non-compliance specifying the details of such noncompliance. If Customer timely provides HackerOne with the required notice, as Customer's sole and exclusive remedy, HackerOne shall re-perform such portion of the Services or otherwise use commercially reasonable efforts to correct any such non-compliance, at its expense, within thirty (30) days of its receipt of such notice. EXCEPT AS SPECIFICALLY SET FORTH HEREIN, THE SERVICES ARE PROVIDED BY HACKERONE "AS IS," WITHOUT WARRANTY OF ANY KIND. WITHOUT LIMITING THE FOREGOING, HACKERONE EXPLICITLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING, CUSTOM OR USAGE OF TRADE. HackerOne makes no warranty that the Services will meet Customer's specific requirements or be available on an uninterrupted, secure or error-free basis.

9. LIMITATION OF LIABILITY. NEITHER CUSTOMER NOR HACKERONE WILL BE LIABLE FOR ANY INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, LOSS OF DATA OR GOODWILL, SERVICE INTERRUPTION, COMPUTER DAMAGE OR SYSTEM FAILURE OR THE COST OF SUBSTITUTE SERVICES ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR FROM THE USE OF OR INABILITY TO USE THE SERVICES, WHETHER BASED ON WARRANTY, CONTRACT, TORT (INCLUDING NEGLIGENCE), OR ANY OTHER LEGAL THEORY, AND WHETHER OR NOT SUCH PARTY HAS BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY. TO THE FULLEST EXTENT PERMITTED BY LAW, IN NO EVENT WILL CUSTOMER'S OR HACKERONE'S TOTAL LIABILITY TO THE OTHER ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR FROM THE USE OF OR INABILITY TO USE THE SERVICES EXCEED THE TOTAL OF THE AMOUNTS PAID BY CUSTOMER TO HACKERONE FOR USE OF THE SERVICES. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH RESULTING FROM LICENSOR'S NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

10. COMPLIANCE WITH LAWS. Each party shall comply with all Applicable Laws in connection with the performance of its obligations and the exercise of its rights under these Terms.

11. PUBLICITY. Except for information that is already made public by Customer through the Customer's Programs and Program Materials and except as may be required by law, neither party shall make any public announcement or conduct any advertising or public relations regarding these Terms unless mutually agreed by the parties. With the Customer's prior written consent (which consent may be withdrawn at any time) and to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71, HackerOne may refer to Customer as a customer on its website and utilize Customer's logo for such purpose.

12. TERM AND TERMINATION. These Terms shall continue in effect for the subscription period of the Services purchased by the Customer. The Customer may terminate these Terms and the applicable subscription if HackerOne fails to cure a material breach of hereof or thereof within thirty (30) days after receiving written notice of the breach from the Customer. When the Customer is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, HackerOne shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer. Upon any termination or expiration of these Terms or the subscription period of the Services purchased, Customer shall be entitled to a refund of any unused Reward prepayment.

13. GOVERNING LAW. This Agreement and any action related thereto will be governed by the Federal laws of United States. The United Nations Convention on Contracts for the International Sale of Goods does not apply to the transactions contemplated by these Terms. The Uniform Computer Information Transactions Act ("***UCITA***") will not apply to these Terms regardless of when and howsoever adopted, enacted and further amended under the governing state laws.

14. GENERAL. To the extent of any conflict between these Terms and any of the HackerOne policies or documents linked to or referenced in these Terms, the terms of these Terms shall govern and control. During the Term, HackerOne shall provide notice to Customer of any material changes to any such linked policies or documents and shall not alter any such policies or documents in any way that would derogate or degrade in any way the Services or modify any of its obligations to Customer hereunder. Any waiver, modification or amendment of any provision of these Terms will be effective only if in writing and signed by duly authorized representatives of both parties. Any terms and conditions contained in any Customer purchase order that are inconsistent with or in addition to the terms and conditions of these Terms will be deemed stricken from such purchase order, unless expressly agreed to in writing by HackerOne. If any provision of these Terms is held to be invalid, prohibited or otherwise unenforceable by legal authority of competent jurisdiction, the other provisions of the Agreement shall remain enforceable, and the invalid or unenforceable provision shall be deemed modified so that it is valid and enforceable to the maximum extent permitted by law. Customer shall not use the Services, or any portion thereof, for the benefit of any third party or in any manner not permitted by these Terms. Any notices or other communications provided by HackerOne under these Terms will be given via email or by posting to the HackerOne Site.

Exhibit A
Services Description

HackerOne provides the HackerOne Platform that allows its customers to gain access to Finders and leverage the Finders to, among other things, find security vulnerabilities on the various systems or scope as set forth in the customer's Program Policy or to perform such other tasks as may be set forth in the customer's Program Policy or agreed to by the customer and the Finders. Finders are independent contractors, not HackerOne's employees or consultants. Programs can be run in private mode where only invited Finders will be notified of the existence of such Program and are permitted to participate in the Program. Depending on the Services purchased from HackerOne, HackerOne may perform or assist in performing various vetting of the Finders before invitations are sent out to Finders for private Programs. The Programs can also be run in public mode, in which case all Finders on the HackerOne Platform are notified the existence of the Program, no specific invitation is needed, and any Finder who meets the condition set forth on the Program Policy will be eligible to participate in the Program. Finders do their tasks independently using their own systems and resources, and then use the HackerOne Platform to describe and submit Finder Submissions. Because Finders discover the vulnerability and create the Vulnerability Report, unless the customer's Program Policy or the details of the specific Services provide otherwise, the intellectual property of the Vulnerability Report belongs to the submitting Finder. Typically, the Finder grants via Finder Terms and Conditions or the customer's Program Policy the necessary license right, free of charge, to allow HackerOne and HackerOne's customer to use the Finder Submissions via the HackerOne Platform, including use via the HackerOne API and integrations with third party tools. All Finders on the HackerOne Platform agree to the HackerOne Finder Terms and Conditions as well as the HackerOne Privacy Policy and the default Disclosure Guidelines when the Finder joins the HackerOne Platform. However, any customer can have its own Program Policy that may be different from or supplement the HackerOne's default Disclosure Guideline and which may set any rules or requirements the customer desires to impose on Finders participating in its Program. When there is a difference between a customer's Program Policy and the default Disclosure Policy or the Finder Terms and Conditions, the Program Policy will govern. HackerOne may also process Reward payments on behalf of a customer after a monetary Reward is awarded under a Program. When a Finder initially signs up on HackerOne Platform, only username and email address are collected. When a Reward is awarded and before payment is processed by HackerOne, HackerOne first requires the Finder to fill out an appropriate tax form, which collects necessary personal data per IRS tax forms. HackerOne checks to make sure the tax form appears valid, and then uses the information from the tax form to perform an OFAC check. If the Finder passes the OFAC check, and payment preference and payment information are supplied, HackerOne will process the payment to the Finder according to the Finder designated payment preference. If the Finder fails the OFAC check, the customer is informed, and the customer and HackerOne will decide jointly the subsequent actions to take.

If purchased by a customer, HackerOne may also provide report management/triage Services, in which HackerOne views the information contained in a Vulnerability Report and performs a series of activities, including attempting to reproduce and validate the vulnerability submitted by the Finder, communicating to Finders, and (if applicable) performing activities on the customer's systems as part of reproducing and validating the vulnerability. HackerOne utilizes staff augmentation contractors to provide such Services. Each such contractor has agreed to confidentiality obligations at least as protective of the Vulnerability Report as HackerOne is subject to under these Terms and HackerOne remains fully liable for all acts or omissions of any such contractors in performing the report management/triage Services. By purchasing such Services, Customer consents to HackerOne's access to and use of the Vulnerability Reports for the purpose of providing such Services and to the use of such staff augmentation contractors.

Exhibit B
Service Level Agreement

This is the Service Level Agreement (this "SLA") by HackerOne for the HackerOne Platform and the associated Services HackerOne provides to its customers who pay for the HackerOne Platform and/or for the Services including all HackerOne Enterprise and Professional offerings. This SLA is not intended for customers who use the HackerOne Platform for free, nor for Finders.

1. Service Level Agreement. HackerOne commits to provide a level of service for the HackerOne Platform demonstrating:

1.1 Platform Uptime. The HackerOne Platform will be operational and available to customers 24 hours per day, 7 days per week at least 99.5% of the time in any calendar month, except for scheduled maintenance and upgrades, and excluding API interruptions or third party system interruptions. HackerOne shall provide at least 24 hours' advance notice to Customer on scheduled maintenance in excess of 30 minutes. Notice will be delivered via electronic means including via the HackerOne Platform.

1.2 Severity Levels and First Response Time. HackerOne Platform software defects/errors will be classified by the reporting party in accordance with the following severity incident guidelines. HackerOne will respond to Customer and provide a First Response in accordance with the time requirements set forth in the table below. "First Response" means a written electronic response from HackerOne to the customer regarding a reported or discovered error acknowledging receipt. Response may be delivered via the HackerOne Platform.

Incident Severity Level	**Definition**	**SLA for Customers on Enterprise Product Edition**	**SLA for Customers on Professional Product Edition**
Severity 1	A critical problem with the HackerOne Platform software in which any of the following occur: the entire services are down, inoperable, inaccessible or unavailable, the entire services otherwise materially cease operation.	2 business hours	4 business hours
Severity 2	A problem with the HackerOne Platform software in which any of the following occur: the services are severely limited or degraded, major functions are not performing properly, the situation is causing a significant impact to certain portions users' operations or productivity.	4 business hours	8 business hours (1 business day)
Severity 3	A problem with the HackerOne Platform software in which any of the following occur: the problem is an irritant, affects non-essential functions, has minor impact to business operations; the problem is localized or has isolated impact; the problem is an operational nuisance.	1 business days	3 business days

1.3. Report Management/Triage Services SLA. HackerOne provides report management, or triage, services for customers who have purchased such Services. Triage Services include validating the Vulnerability Reports submitted by Finders. HackerOne commits to the following First Response timelines for the triage Services it performs for its customers:

- Triage First Response to customers generally: 2 business days
- Triage First Response for Enterprise tier customers: 1 business day

2. SLA Exclusions. This SLA and any applicable Service Levels do not apply to any performance or availability issues:

(a) Due to factors outside HackerOne's reasonable control;

(b) That resulted from the customer's or a third party's (not within HackerOne's control) hardware or software;

(c) That resulted from actions or inactions of the customer (or the customer's employees, agents, contractors, or vendors gaining access to HackerOne's Service by means of the customer's authorized users' accounts or equipment) or third parties not within HackerOne's control;

(d) Caused by the customer's use of the Service after HackerOne advised the customer to modify its use of the Service, if the customer did not modify its use as advised; or

(e) During any beta, pre-release and/or trial Services.

3. Service Credit Claims.

3.1 In the event HackerOne fails to deliver against the service levels as described above (an "Incident"), the sole and exclusive remedy for such failure shall be in the form of service credit to the customer. If the Service fails to meet the above service levels, a customer can file a claim to and will receive a service credit equal calculated in accordance with Section 4 of this SLA.

3.2 In order to be eligible to submit a claim for a service credit (a "Claim") with respect to any Incident, the customer must first have notified HackerOne's Customer Support of the Incident, using the procedures set by HackerOne, within five business days following the Incident.

3.3 To submit a Claim, the customer must submit, by the end of the calendar month following the month in which the Incident occurred, the Claim to claims@hackerone.com and provide to Customer Support all reasonable details regarding the Claim, including but not limited to, detailed descriptions of the Incident(s), the duration of the Incident, network traceroutes, the URL(s) affected and any attempts made by the customer to resolve the Incident.

3.4 HackerOne will use the information submitted and all information reasonably available to it to validate Claims and make a good faith judgment on whether a service credit is due with respect to such Claims.

4. Service Credits. Service credits are a customer's sole and exclusive remedy for any violation of this SLA. Service credits are provided in the form of a no charge subscription extension and will only be calculated as set forth below.

Outage in a Month (Minutes)	**Service Credit in Subscription Extension**	**Comments**
< 216 Minutes	0	This is for 99.5% platform uptime
217 – 500 Minutes	One week	Customer subscription will be extended by one week
500 – 1,000 Minutes	Two weeks	Customer subscription will be extended by two weeks
>1,000 Minutes	Four weeks	Customer subscription will be extended by four weeks

Exhibit C
Current Version of Vulnerability Disclosure Guidelines

All technology contains bugs. If you've found a security vulnerability, we'd like to help out. By submitting a vulnerability to a program on HackerOne, or signing up as a Security Team, you acknowledge that you have read and agreed to these guidelines.

VULNERABILITY DISCLOSURE PHILOSOPHY

Finders should...

- **Respect the rules.** Operate within the rules set forth by the Security Team, or speak up if in strong disagreement with the rules.
- **Respect privacy.** Make a good faith effort not to access or destroy another user's data.
- **Be patient.** Make a good faith effort to clarify and support their reports upon request.
- **Do no harm.** Act for the common good through the prompt reporting of all found vulnerabilities. Never willfully exploit others without their permission.

Security Teams should...

- **Prioritize security.** Make a good faith effort to resolve reported security issues in a prompt and transparent manner.
- **Respect Finders.** Give finders public recognition for their contributions.
- **Reward research.** Financially incentivize security research when appropriate.
- **Do no harm.** Not take unreasonable punitive actions against finders, like making legal threats or referring matters to law enforcement.

Safe Harbor

We are committed to protecting the interests of Finders. However, vulnerability disclosure is an inherently murky process. The more closely a Finder's behavior matches these guidelines, the more we'll be able to protect you if a difficult disclosure situation escalates.

Submission Process

Security Teams will publish a program policy designed to guide security research into a particular service or product. You should always carefully review this program policy prior to submission as they will supersede these guidelines in the event of a conflict.

If you believe you have found a vulnerability, please submit a Report to the appropriate program on the HackerOne platform. The Report should include a detailed description of your discovery with clear, concise reproducible steps or a working proof-of-concept. If you don't explain the vulnerability in detail, there may be significant delays in the disclosure process, which is undesirable for everyone.

The Report will be updated with significant events, including when the vulnerability has been validated, when more information is needed from you, or when you have qualified for a bounty.

Vulnerability Disclosure Process

The contents of the Report will be made available to the Security Team immediately, and will initially remain non-public to allow the Security Team sufficient time to publish a remediation. After the Report has been closed, Public disclosure may be requested by either the Finder or the Security Team.

- **Default:** If neither party raises an objection, the contents of the Report will be made public within 30 days.
- **Mutual agreement:** We encourage the Finder and Security Team members to remain in open communication regarding disclosure timelines. If both parties are in agreement, the contents of the Report can be made public on a mutually agreed timeline.
- **Protective disclosure:** If the Security Team has evidence of active exploitation or imminent public harm, they may immediately provide remediation details to the public so that users can take protective action.
- **Extension:** Due to complexity and other factors, some vulnerabilities will require longer than the default 30 days to remediate. In these cases, the Report may remain non-public to ensure the Security Team has an adequate amount of time to address a security issue. We encourage Security Teams to remain in open communication with the Finder when these cases occur.
- **Last resort:** If 180 days have elapsed with the Security Team being **unable or unwilling to provide a vulnerability disclosure timeline**, the contents of the Report may be publicly disclosed by the Finder. We believe transparency is in the public's best interest in these extreme cases.

Private Program

Some Finders may receive invitations to private Programs. Your participation in a private Program is entirely optional and subject to strict non-disclosure by default. Prior to accepting an invitation to a private Program, Finders should carefully review any program policies and non-disclosure agreements required for participation. Finders that intend any form of public disclosure should not participate in private Programs.

HackerOne recommends two alternatives:

(a) Submit directly to the Security Team outside of the Program. In this situation, Finders are advised to exercise good judgement as any safe harbor afforded by the Program Policy may not be available.

(b) Utilize our disclosure assistance process.

Public Recognition

You may receive public recognition for your find if 1) you are the first person to file a Report for a particular vulnerability, 2) the vulnerability is confirmed to be a valid security issue, and 3) you have complied with these guidelines. If a Finder prefers to remain anonymous, we encourage them to submit under a pseudonym.

Bug Bounty

Some Security Teams may offer monetary rewards for vulnerability disclosure. Not all Security Teams offer monetary rewards, and the decision to grant a reward is entirely at their discretion. The amount of each bounty payment will be determined by the Security Team. Bounty payments are subject to the following eligibility requirements:

- Because we're based in the United States, we aren't able to pay bounties to residents or those who report vulnerabilities from a country against which the United States has trade restrictions or export sanctions as determined by the U.S. Office of Foreign Assets Control (OFAC).
- Minors are welcome to participate in the program. However, the Children's Online Privacy Protection Act restricts our ability to collect personal information from children under 13, so you will need to claim your bounties through your parent or legal guardian if you are 12 or younger.
- All payments will be made in U.S. dollars (USD) and will comply with local laws, regulations and ethics rules. You are responsible for the tax consequences of any bounty you receive, as determined by the laws of your country.
- It is your sole responsibility to comply with any policies your employer may have that would affect your eligibility to participate in this bounty program.

Definitions

Security Team: A team of individuals who are responsible for addressing security issues found in a product or service. Depending on the circumstances, this might be a formal security team from an organization, a group of volunteers on an open source project, or an independent panel of volunteers (such as the Internet Bug Bounty).
Finder: Also known as hackers. Anyone who has investigated a potential security issue in some form of technology, including academic security researchers, software engineers, system administrators, and even casual technologists.
Report: A Finder's description of a potential security vulnerability in a particular product or service. On HackerOne, Reports always start out as non-public submissions to the appropriate Security Team.
Vulnerability: A software bug that would allow an attacker to perform an action in violation of an expressed security policy. A bug that enables escalated access or privilege is a vulnerability. Design flaws and failures to adhere to security best practices may qualify as vulnerabilities. Weaknesses exploited by viruses, malicious code, and social engineering are not considered vulnerabilities unless the Security Team says otherwise in the program's policy.
Programs: Security Teams may publish a Program and Program Policy designed to guide security research into a particular service or product. If this program is private, your participation is entirely optional and subject to non-disclosure by default.
Contact
HackerOne is always open to feedback, questions, and suggestions. If you would like to talk to us, please feel free to email us at support@hackerone.com or follow us on Twitter @hacker0x01.
Changes to These Guidelines
We may revise these guidelines from time to time. The current version is 1.2, updated on July 29, 2019 will always be at https://www.hackerone.com/disclosure-guidelines. If we make changes that we believe will substantially alter your rights, we will email you and prominently display a notice on our site 7 days before we make those changes.

Exhibit D
Current Version of Privacy Policy

Effective as of April 12, 2021, HackerOne Inc. and its affiliates (collectively, "HackerOne", "we", "us", or "our") have updated our Privacy Policy.
Your data is just that, **YOUR** data. HackerOne is committed to ensuring the privacy of your data. We are further committed to preventing unauthorized access to that data. Our Privacy Policy details what data is collected from our Customers and Finders, how we use it, and how it is stored.

1. WHO WE ARE

HackerOne is an industry leader in hacker-powered security. HackerOne partners with the global security researcher community, which may be referred to as hackers or Finders (we will use the term Finder(s) for the purposes of our Privacy Policy), to provide businesses with access to top talent Finders who identify and surface relevant security issues in a business's products or services. HackerOne operates a bug bounty & vulnerability disclosure software-as-a-service platform known as the HackerOne Platform, the website located at hackerone.com and related domains and subdomains, and related services, including live hacking events, marketing, and customer service and ancillary support services (collectively referred to as "Services"). HackerOne is a Delaware corporation headquartered in San Francisco, California with offices currently in London and the Netherlands.

We respect your privacy and take safeguarding your data seriously. Please read this Privacy Policy carefully together with the General Terms and Conditions ("Terms") available at https://www.hackerone.com/terms/general, which governs your use of the Services, to understand what Personal Information (defined below) we collect from you, how we use it, and your choices related to our use of your Personal Information. By using the Services, you acknowledge our collection, use, disclosure, and retention of your personal information as described in the Privacy Policy. If you do not agree with the terms of this Policy, please do not use the Services.

2. WHAT IS PERSONAL INFORMATION?

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

3. WHERE IS (Y)OUR INFORMATION STORED?

As a global company we understand that there are many different privacy and data protection laws where our Customers and Finders are based. We know and understand the value of your information. We will take all reasonable steps to ensure that your Personal Information is treated securely and in accordance with the laws and regulations relevant to where you are located.

We are a company headquartered in California and so, our Sites and Servers are hosted here in the United States. Therefore, the Personal Information that we collect from you will be received, transferred and/or stored in the United States.

If you are located outside the United States, please see our section on International Data Transfer below.

4. PERSONAL INFORMATION WE PROCESS

We process Personal Information that you actively submit to us, that we automatically collect through your use of our Services, and that we collect from third-parties for the following reasons We may, when securing our website and Services, collect details about your device, your computer's internet protocol (IP addresses) and other technical information, through our data security and firewall providers and/or when marketing our Services, we may collect identity and contact data from publicly available sources. For compliance with applicable laws (including but not limited to anti-money laundering and financing laws and regulations), we may through third parties who use verification providers or due diligence, and screening information providers verify your information and collect information from publicly available sources or check data against government sanction lists.

We may process your Personal Information with or without automatic means, including 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 of your Personal Information.

We <u>DO NOT</u> sell the Personal Information we collect to other parties.

4.1 Personal Information that you actively submit to us.

We collect Personal Information that you actively submit to us through your account, website forms, email subscriptions, surveys, events, conferences, customer service and ancillary support services , inquiries, and other interactions. You will normally know when we collect your Personal Information because we will directly ask you for the information. Examples are provided below. We will require certain Personal Information in order for you to use our Services or for us to be able to contact you. There may also be circumstances where providing Personal Information is optional and does not impact your access to Services.

4.1.1 Your Account. Whether you are a Customer or a Finder (or both), when you create a HackerOne account, you are required to provide us with profile information, including your email address and password. HackerOne stores this information to help identify you when you log in. Once you've registered, you create a user profile. Your profile information includes your name (if you choose to provide it), chosen username, company name (if applicable), and if you choose, a profile photo, your location, your social media and other third-party affiliations, and any other information you include in the "About me" or "Intro" fields. We may display your profile information on our site where other users of the Services and visitors to

our website will be able to see that information. If you enable two-factor authentication, we will store a phone number used for account recovery purposes.

If you are a Customer, in addition to your profile information, you may provide us with financial information, such as your credit card or debit card information or your banking information, in order to assist us in awarding bounties, collecting bounty deposits, or collecting HackerOne fees.

If you are a Finder, in addition to your profile information, you may need to provide us with other personally identifying information necessary for background and fraud checking purposes where required. This includes your date of birth, nationality, current and previous addresses, your social security number (or tax identification number), and for Reward purposes, your banking, Coinbase, PayPal, or similar information in order to allow us to pay you monetary Rewards from Customers. In addition, in order that we can award any "swag" where available, we may ask for information such as a mailing address, telephone number, and clothing size. In addition to Personal Information we collect, your profile may be publicly associated with any vulnerability reports or other content that you submit, in the event these are published on the Services.

4.1.2 Events. We host events to bring together industry professionals in a casual setting. We also host live hacking events where top Finders from all over the globe join together to find vulnerabilities on HackerOne Customer programs. To register in advance for these events, we may collect your first name, last name, email address, company name (if applicable), job title (if applicable), and give you an option to provide us a website reference.
4.1.3 Email Subscriptions. We actively communicate with subscribers through newsletters, webinars, and education content, and also send emails about product updates, events, the status of the HackerOne Platform, and updates to the third-party service providers (sub-processors) used to process Personal Information. A subscriber may be required to provide their email address and other contact information to receive communications.
4.1.4 Text Subscriptions. We may communicate with subscribers through text messages concerning the status of the HackerOne Platform. A subscriber is required to provide their phone number to receive texts.
4.1.5 Recruitment. We are always looking out for new employees. So should you decide to apply to us (or a partner recruitment provider or service) for a role, we will collect the information contained in your resume/cv, (information such as where you went to school or previous employment) along with any other relevant information you choose to provide to us.
4.1.6 Surveys. We occasionally conduct surveys in order to gather data central to assessing our business objectives and understanding the Finder community. Participation in surveys is always optional. Information provided in surveys is anonymized and aggregated for analysis.
4.1.7 Contact Us. There are multiple opportunities for you to contact us, including for support, to report a bug, make a suggestion, make a sales inquiry, request a product demonstration, request research, and for customer service and ancillary support services. Online forms collect Personal Information such as a first name, last name, email address, company (if applicable), job title (if applicable), reason for contact, and may provide an option to attach a file. When we contact you in response to your request, we may collect additional Personal Information.
4.2 Personal Information we automatically collect through your use of the Services.
We receive some Personal Information automatically when you visit HackerOne Services. This includes information about the device, browser, and operating system you use when accessing our site and Services, your IP address, the website that referred you, which pages you request and visit, and the date and time of each request you make. If you visit the HackerOne Platform when you are logged into your account, we also collect the user identification number we assign you when you open your account.

4.3 Personal Information we collect from third-party sources.
We are continually expanding our Customer reach. As part of our business-to-business marketing, we collect Personal Information from third-party sources to identify individuals who hold relevant job roles in key industries. Personal Information collected generally includes a first name, last name, job title, company name, email address, and phone number. We generally communicate via email or telephone to provide information about HackerOne programs and offer businesses an opportunity to try out HackerOne Services.

4.4 Personal Information of minors.
We welcome all Finders to register a HackerOne account as a Finder, participate in our programs, and submit reports to HackerOne. We believe that skilled Finders are not determined by age. However, applicable laws may restrict our ability to collect Personal Information from minors unless we have first obtained the consent of the minor's parent or guardian. Please note that the definition of a minor varies by jurisdiction and various laws institute age related requirements. If you are considered a minor and want to submit a vulnerability report to us, please ask your parent or guardian to submit it for you. Please note that in addition, any Reward payments that may apply are only issued to an adult. HackerOne does not otherwise knowingly collect Personal Information of minors, and the HackerOne Services are not directed to minors. If we become aware that we have collected Personal Information from a minor in conflict with applicable law, we will delete that information or obtain the requisite consent from the minor's parent or guardian.

4.5 Personal Information we collect using cookies and similar tracking technologies.
We (and the third-party service providers working on our behalf) use various technologies to collect Personal Information. This may include saving cookies to your device, using pixels and similar technologies. For information on what cookies and pixels are, which ones we use, why we use them, and how you can manage their use, please see our Cookies Policy, which provides more information about how and why we or our commercial partners may process certain personal data relating to you, and should be read in conjunction with this privacy policy.

5. HOW WE USE YOUR PERSONAL INFORMATION
We use your Personal Information to operate our Services, fulfill our contractual obligations in our contracts with Customers and Finders or take steps preparatory to entering into those contracts, to review and enforce compliance with our Terms, guidelines, and policies, to analyze the use of the Services in order to understand how we can improve our content and service offerings and products, and for administrative and other business purposes. We process Personal Information for sales leads, subscription services, payments, employee training, marketing, data analysis, security monitoring, auditing, research, and to comply with applicable laws, to exercise legal rights, and meet tax and other regulatory requirements.

In this context, the legal basis for our processing of your Personal Information is either the necessity to perform or enter into contractual and other obligations, our legitimate business interests as a provider of security services (and the other legitimate interests described above), compliance with legal and regulatory requirements, or in some instances your consent.

6. SHARING OF PERSONAL INFORMATION
WE DO NOT SELL YOUR PERSONAL INFORMATION!
We may share your Personal Information in the following circumstances:

6.1 Third-party Service Providers.
We may share information we collect about you with third-party service providers to perform tasks on our behalf in supporting the Services. The types of service providers, or sub-processors, to whom we entrust Personal Information include: (i) payment providers; (ii) providers of hosting services; (iii) sales and marketing providers; (iv) providers of document and content management tools; (iv) providers of analytic data services; and (v) other services such as system support, subscription services, verification, and ticketing.

6.2 Customers.
For Finders who participate in certain Customer programs, to the extent described in the policies of such Customer programs, HackerOne may share contact information about those Finders (for example, name, company name (if applicable), and email address) to allow those Customers to contact those Finders to allow them to interact directly or as otherwise authorized by the Finder with respect to the specific Customer program or service. For Finders who choose to submit a vulnerability report directly to a Customer outside the HackerOne Platform, HackerOne may provide that Customer with a reference to your public profile information. In the event of a serious security concern, HackerOne may determine, in its sole discretion, that Personal Information will be shared with a Customer to identify and resolve the security concern.

6.3 Regulatory Bodies, Public Authorities, and Law Enforcement.
We may access and disclose your Personal Information to regulatory bodies if required under applicable law or regulation. This may include submitting Personal Information required by tax authorities. We may disclose your Personal Information in response to lawful requests by public authorities or law enforcement, including to meet national security or law enforcement requirements. If we are going to release your Personal Information in this instance, our policy is to provide you with notice unless we are prohibited from doing so by law or court order (including orders under 18 U.S.C. § 2705(b)).

6.4 Merger, Sale, or Other Asset Transfers.
If we are involved in a merger, acquisition, financing due diligence, reorganization, bankruptcy, receivership, sale of company assets, or transition of service to another provider, then your Personal Information may be disclosed or transferred as part of such a transaction as permitted by law and/or contract. Should such an event occur, HackerOne will endeavor to direct the transferee to use Personal Information in a manner that is consistent with the Privacy Policy in effect at the time such Personal Information was collected.

6.5 Other Disclosures.
Where there is agreement by Customers and Finders that Finder Submissions are publicly disclosed, then certain information about the submission associated with your profile may be published through our Services. We may share Personal Information with our affiliated companies. We may also disclose your Personal Information to exercise or defend legal rights; to take precautions against liability; to protect the rights, property, or safety of HackerOne, other users of our Services, of any other individuals, or of the general public; to maintain and protect the security and integrity of our Services or infrastructure; to protect HackerOne and our Services from fraudulent, abusive, or unlawful uses; or to investigate and defend HackerOne against third-party claims or allegations. Disclosures may be made to courts of law, attorneys and law enforcement, or other relevant third parties in order to meet these purposes.

Please note that we share aggregated information and non-identifying information with third parties for industry research and analysis, demographic profiling, and other similar purposes. In addition, our Services may contain links to other websites not controlled by us, and these other websites may reference or link to our Services; we encourage you to read the privacy policies applicable to these other websites.

5.6 California Consumer Privacy Act of 2018 ("CCPA").
Pursuant to §§ 1798.110 and 1798.115 of the CCPA, the categories of Personal Information we have **collected about consumers and disclosed about consumers for a business purpose** in the preceding 12 months are:

- Identifiers such as a real name, alias, postal address, email address, unique personal or online identifier, Internet Protocol address, account name, SSN, driver's license or passport number, or other similar identifiers;
- Other information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including signature, bank account number, credit card number, debit card number, or any other financial information;
- Commercial information, including products or services purchased, obtained, or considered; other purchasing or consuming histories or tendencies;
- Internet or other electronic network activity information, including, browsing history, search history, and information regarding a consumer's interaction with an internet website, or advertisement;
- Professional or employment-related information; and
- Inferences drawn from any of the information identified to create a profile about a consumer reflecting the consumer's preferences, intelligence, abilities, and aptitudes (applies only to Finders who have registered an account and participate in programs and subsequent skill ratings).
-

Please note that not all of this information is collected or disclosed from all consumers using our Services.

7. RETENTION OF PERSONAL INFORMATION

HackerOne retains Personal Information for a reasonable time period to fulfill the processing purposes mentioned above. Personal Information is then archived for time periods required or necessitated by legal or regulatory considerations. When archival is no longer required, Personal Information is deleted from our records.

You may choose to disable your HackerOne account at any time. This means your user profile will no longer be visible on the Services. However, for the purposes mentioned above, we may need to retain information within our internal systems. In addition, public vulnerability reports and associated information that you have submitted will still be available on the Services.

We retain Personal Information that we are required to retain to meet our regulatory obligations including tax records and transaction history. We regularly review our retention policies to ensure compliance with our obligations under data protection laws and other regulatory requirements. We regularly audit our databases and archived information to ensure that Personal Information is only stored and archived in alignment with our retention policies.

8. PROTECTION OF PERSONAL INFORMATION

HackerOne uses technical and organizational measures to protect the Personal Information that we store, transmit, or otherwise process, against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. We regularly consider appropriate new security technology and methods as we maintain and develop our software and systems.

However, you should keep in mind that the Services are run on software, hardware, and networks, any component of which may, from time to time, require maintenance or experience problems or breaches of security beyond our control. Please also be aware that despite our best efforts to ensure the security of your data, we cannot guarantee that your information will be 100% secure.

Please recognize that protecting your Personal Information is also your responsibility. We urge you to take every precaution to protect your information when you are on the Internet, such as using a strong password, keeping your password secret, and using two-factor authentication. If you have reason to believe that the security of your account might have been compromised (for example, your password has been leaked), or if you suspect someone else is using your account, please let us know immediately.

9. INTERNATIONAL DATA TRANSFER

If you are located outside the United States and choose to provide your Personal Information to us, we will transfer your Personal Information to (or receive it in) the United States and process it there. Your Personal Information may be transferred to, and maintained on, computers located outside of your state, province, country, or other governmental jurisdiction where the privacy laws may not be as protective as those in your jurisdiction. Whenever we transfer your Personal Information, we will take all reasonable steps to ensure that your privacy rights continue to be protected. Wherever you are based, we are responsible for the processing of your Personal Information, including any subsequent transfers to third parties.

9.1 EU - US Data Transfers

If HackerOne transfers Personal Information to a jurisdiction (or to a third party in a jurisdiction) for which the European Commission, Switzerland or the UK (as applicable) has not issued an adequacy decision, HackerOne will implement appropriate technical and security safeguards as required, including Standard Contractual Clauses (see below) approved by competent authorities, to transfer Personal Data in accordance with data protection and privacy laws, either internally between our group entities, or between us and our Finders and Customers (such as where we process personal data on their behalf).

9.2 Standard Contractual Clauses

In order to comply with the transfer of data rules between the US and the UK, Switzerland or EU we offer Standard Contractual Clauses (sometimes also referred to as EU Model Clauses). Standard Contractual Clauses are contractual clauses designed to ensure HackerOne meets the legal and regulatory requirements for Customers and Finders using the Services in the European Economic Area (“EEA”), Switzerland and the UK. A copy of our standard Data Processing Agreement which incorporates the Standard Contractual Clause is available here.

Much like our Privacy Policy, should you or others (on whose behalf you lawfully share Personal Information) be located in the EEA, Switzerland or the UK and use the Services, all parties will be deemed to have accepted these Standard Contractual Clauses. HackerOne is committed to safeguarding Personal Information and will always undertake to meet the approved safeguards and findings of adequacies, under all applicable data protection and privacy laws. Please let us know if you would like more information about the measures we have in place.

10. PRIVACY RIGHTS

Subject to where you are based you may have rights under data protection and privacy laws, including but not limited to the CCPA and the EU General Data Protection Regulation (“GDPR”). Under these laws, individuals have the right to access Personal Information and to correct, amend, restrict, or delete that information where it is inaccurate, or has been processed in violation of your rights, except in some cases where their request is manifestly unfounded or excessive, or where certain other circumstances apply, for example where the rights of persons other than the individual will be violated.

If you have a HackerOne account, we rely upon you to keep your information up to date. You may edit your profile information and may also choose to disable your HackerOne account at any time through your account settings. For subscription services, such as newsletters, webinars, events, and the like, we offer you the ability to manage your preferences and choose whether to receive email communication for each service. To manage your preferences, please visit the Email Subscription Preference Center at https://ma.hacker.one/SubscriptionManagement.html. Where you are receiving communication from us of a marketing nature, we provide the ability for you to unsubscribe directly from the email.

Where we rely upon consent as a legal basis for processing, you may withdraw your consent at any time. Please note the withdrawal of your consent does not affect the lawfulness of processing based on consent before withdrawal.

Individuals in the many territories where we operate have certain rights that may be subject to limitations and/or restrictions. These include but are not limited to, the right to: (i) request access to and rectification or erasure of their Personal Information; (ii) obtain restriction of processing or to object to processing of their Personal Information; and (iii) ask for a copy of their Personal Information to be provided to them, or a third party, in a digital format. If you wish to exercise one of the above-mentioned rights, please send us your request to the contact details set out below. Individuals also have the right to lodge a complaint about the processing of their Personal Information with their local data protection authority.

Personal Information subject rights under the CCPA may also apply to certain individuals and households. These rights include the right to: (i) know what Personal Information is being collected about them, (ii) know whether their Personal Information is sold or disclosed at to whom, (iii) say no to the sale of Personal information, (iv) access their Personal Information, and (v) equal service and price, even if they exercise their privacy rights.

10.1 Exercising your rights and Privacy Disputes
You may also contact us with your Personal information inquiries or for assistance in modifying or updating your Personal Information and to exercise any additional applicable statutory rights. We respect the privacy of all individuals and invite you to submit your requests, irrespective of where you reside. Our contact details are provided at the end of this Privacy Policy.

11. CHANGES TO THIS POLICY
We may modify this Privacy Policy from time to time, which will be indicated by changing the date indicated at the top of this page. The most current version of the Privacy Policy will govern our use of your Personal Information and will always be at https://www.hackerone.com/privacy. If we make changes that we believe will substantially alter your rights, we will notify you by email (sent to the email address specified in your HackerOne account), by means of a notice on our Services prior to the change becoming effective, or as otherwise required by law. In certain cases, we may also seek your consent to further use of your Personal Information where this is required.

12. CONTACT INFORMATION
If you would like to contact us with questions or concerns about this Privacy Policy, our privacy practices, or would like to exercise your privacy rights, you may contact us via any of the following methods:

Email: privacy@hackerone.com
Toll-free Number (USA): +1 (855) 242-8699

Mailing Address:

Attn: Privacy Officer
HackerOne Inc.
548 Market Street, PMB 24734
San Francisco, CA 94104-5401
United States of America

Our EU representative:

Attn: Privacy Officer
HackerOne B.V.
Griffeweg 97/4
9723 DV Groningen
The Netherlands

Exhibit E
Current Version of Data and Information Security Terms

Last Updated: February 16, 2021
Certain capitalized terms used in this document are defined in the General Terms and Conditions found at https://www.hackerone.com/terms/general, which are incorporated by reference. This document shall form a part of the Terms.

1. **Policies and Procedures.** HackerOne shall maintain written security management policies and procedures to prevent, detect, contain, and correct violations of measures taken to protect the confidentiality, integrity, and availability of HackerOne information systems and/or Customer's Confidential Information. Such policies and procedures shall (i) assign specific data security responsibilities and accountabilities to specific individual(s); (ii) include a formal risk management program, which includes periodic risk assessments; and (iii) provide an adequate framework of controls that safeguard Customer's information systems, including without limitation any hardware or software supporting Customer, and Customer's Confidential Information.

2. **Security Evaluations.** HackerOne shall engage one or more third parties to periodically (no less than annually) evaluate its processes and systems to ensure continued compliance with obligations imposed by law, regulation, or contract with respect to the confidentiality, integrity, availability, and security of Customer's Confidential Information within HackerOne information systems as well as the maintenance and structure of HackerOne's information systems. The results of these evaluations and any remediation activities taken in response to such evaluations will be documented and available to Customers upon request.

3. **Physical Security.** HackerOne shall maintain appropriate physical security controls (including facility and environmental controls) to prevent unauthorized physical access to HackerOne information systems and areas in which Customer's Confidential Information is stored or processed.

4. **Visitor Access Logs.** HackerOne shall maintain sign in access logs for visitors and guests and ensure that such visitors and guests are escorted while in the facility. In addition, these access logs shall be maintained in a secure location for three (3) months.

5. **Perimeter Controls.** HackerOne shall maintain reasonable network perimeter controls such as firewalls at all perimeter connections. HackerOne shall periodically (no less than annually) evaluate its network perimeter controls.

6. **Vulnerability Management.** HackerOne shall employ reasonable vulnerability management processes to mitigate data security risks to Customer's Confidential Information. These processes shall include mitigation steps to resolve issues identified by HackerOne, Customer, or any regulator, auditor, or other external constituent of either party.

7. **System Hardening.** System configuration parameters shall include procedures to disable all unnecessary services on devices and servers. This practice shall at a minimum be applied to all systems that access, transmit, or store Customer's Confidential Information.

8. **Patch Management.** HackerOne shall establish and adhere to policies and procedures for patching systems. Systems and applications used to access, process or store Customer's Confidential Information shall be maintained at current stable patch level.

9. **Anomaly Detection.** HackerOne shall install commercially reasonable anomaly detection software, to include anomaly / intrusion detections and deviations from standard system configuration, on all systems used to access, process or store Customer's Confidential Information as well as other information that HackerOne hosts. In addition, definition files shall be updated regularly.

10. **Incident Response.** HackerOne shall maintain formal processes to detect, identify, report, respond to, and resolve any event that compromises the confidentiality, availability, or integrity of Customer's data or service provider's systems ("Security Incidents") in a timely manner.

11. **Incident Notification.** HackerOne shall immediately provide Customer with notification of any known or reasonably suspected breach of security relating to Customer Systems or Customer's Confidential Information. HackerOne will notify Customer immediately following discovery of any suspected breach or compromise of the security, confidentiality, or integrity of any Customer's Confidential Information. Written notification provided pursuant to this paragraph will include a brief summary of the available facts and the status of HackerOne's investigation.

12. **System Logs.** For all systems that access, transmit or store Customer's Confidential Information, system logs shall be in place to uniquely identify individual users and their access to associated systems and to identify the attempted or executed activities of such users. All systems creating system logs shall be synchronized to a central time source. Reasonable processes shall be in place to review privileged access and identify, investigate and respond to suspicious or malicious activity. System log trails shall be secured in a manner to prevent unauthorized access, modification, and accidental or deliberate destruction. These logs shall be maintained in accordance with the retention requirements set forth in the Agreement or upon a mutual written agreement signed by both parties.

13. **Background Checks.** HackerOne shall maintain processes to determine whether a prospective member of HackerOne's workforce is sufficiently trustworthy to work in an environment which contains HackerOne information systems and Customer's Confidential Information.

14. **Change Control Process.** HackerOne shall maintain reasonable change control processes to approve and track all changes within HackerOne's computing environment. Substantive changes to the HackerOne production environment require a separate tracking and review process with additional authorizations.

15. **Protection of Storage Media.** HackerOne shall ensure that storage media containing Customer's Confidential Information is properly sanitized of all Customer's Confidential Information or is destroyed prior to disposal or re-use for non-HackerOne processing. All media on which Customer's Confidential Information is stored shall be protected against unauthorized access or modification. HackerOne shall maintain reasonable and appropriate processes and mechanisms to maintain accountability and tracking of the receipt, removal and transfer of storage media used for HackerOne information systems or on which Customer's Confidential Information is stored.

16. **System Accounts.** HackerOne shall maintain appropriate processes for requesting, approving, and administering accounts and access privileges for HackerOne information systems and Customer's Confidential Information. HackerOne personnel, who access systems that store, transmit or process Customer's Confidential Information shall be assigned individual system accounts to ensure accountability for access granted. This information is logged and stored in accordance with HackerOne’s Data Retention guidelines.

17. **Passwords.** HackerOne shall implement appropriate password parameters for systems that access, transmit or store Customer's Confidential Information ("Related Systems"). HackerOne shall implement strong authentication services,complex passwords ("Passwords"), and Multi-factor Authentication (where applicable) for all network and systems access to Related Systems. Default manufacturer passwords used in HackerOne's products shall be changed upon installation.

18. **Third Parties.** HackerOne shall ensure that any agent, including without limitation any third-party subprocessor or subcontractor, to whom HackerOne provides Customer's Confidential Information agrees to maintain reasonable and appropriate safeguards to protect such Customer's Confidential Information.