

ACCESS AND SERVICES AGREEMENT

This Access and Services Agreement (“Agreement”) is entered into this 25th day of September, 2020 (the “Effective Date”) by and between WalkMe, Inc., a Delaware Corporation with offices at 71 Stevenson Street, 20th Floor, San Francisco, CA 94105 (“Service Provider”, “Supplier”, or “WalkMe”), and Comcast Cable Communications Management, LLC, a Delaware limited liability company on behalf of itself and its current and future Affiliates that choose to utilize the Technology and Services, (“Client”, “Customer”, or “Comcast”) (each a “Party” and collectively the “Parties”), and describes the terms and conditions governing Client’s use of Service Provider’s services.

1. Definitions and Exhibits.

a) Besides the terms defined elsewhere in this Agreement, the following terms shall have the following meanings: (i) “**Access(ing)**” means to store data in, retrieve data from, or otherwise make use of (directly or indirectly) data or technology through electronic means; (ii) “**Affiliate**” means, with respect to any legally recognizable entity, any other entity that now or hereafter, directly or indirectly controls, is controlled by or is under common control with such specified entity; (iii) “**Documentation**” means the User instructions and such other instructional information provided by Service Provider for use with the Technology and Services; (iv) “**Exhibit**” means the attached Exhibits agreed to by the Parties subject to the terms of this Agreement; (v) “**Order**” means a license order, order form, statement of work (SOW), or ordering document, hereunder and shall be substantially in the form attached as Exhibit A-1 or Exhibit A-2 hereto, mutually signed by both parties; (vi) “**Services**” means the Access to and utilization of the Technology that Service Provider is providing to Client as contemplated by this Agreement and as further described in Exhibit A as well as any other services (which may include professional services) provided by Service Provider in association with the Technology, as described in Exhibit A or any Order attached to this Agreement; (vii) “**Technology**” means the software underlying the Services; (viii) “**Users**” or “**End Users**” means the individuals for whom the WalkMe code loads, which may include employees, consultants, contractors and other third party service providers of Client using and accessing the Services, Technology, and Documentation. The number of Users shall be as specified in an applicable Order.

b) All Exhibits, schedules, attachments and SOWs referenced in this Agreement are hereby incorporated into this Agreement by such reference.

2. License Grant; Technology Access. Service Provider hereby grants to Client a limited scope, nonexclusive, nontransferable non-sublicensable license to use and Access the Service and Technology modules described in Exhibit A for use by Client and its Users for the duration of the subscription term and in accordance with the User count limitation and other terms set forth in an applicable Order for Client’s business purposes and as further described in Exhibit A and/or in the Documentation during the Term. Client may permit Client’s affiliates, consultants, and contractors to use and Access the Service in accordance with the terms of this Agreement and applicable Order. Client and Users may use the Documentation in association with the licensed use of the Services and Technology. Client shall administer the registration and password access of its Users. Upon expiration of an applicable subscription period of the Order, the applicable Order may be renewed and/or replaced by a new Order.

3. Services Scope.

a) If applicable, Service Provider shall provide the implementation services (“Initial Implementation”), if any, described on the Order Form .

b) Ongoing Support Services. Beginning on the Effective Date, Service Provider shall provide the following ongoing support services to Client:

(i) Service Provider shall provide to Client the telephone assistance and product support as set forth on Exhibit A regarding Client's proper and authorized use of the Technology and access to the Services; and

(ii) Service Provider shall provide to Client, during Service Provider's normal business hours, commercially reasonable efforts in solving production problems that arise in connection with Client's proper and authorized use of the Technology or in correcting any errors reported by Client, in accordance with Exhibit B. Client shall provide to Service Provider reasonably detailed documentation and explanation, together with underlying data, to substantiate any error and to assist Service Provider in its efforts to diagnose, reproduce and correct the error. These support services shall be provided by Service Provider remotely. In the event that support services need to be provided by Service Provider at Client location(s) Service Provider and Client agree that on-site services are necessary to diagnose or resolve the problem, subject to fees and expenses to be mutually agreed upon between the Parties, in an amendment to this Agreement.

c) Service Provider shall provide the Services to Client in keeping with the Service Level Agreement set forth in Exhibit B.

d) At Client's reasonable request, Service Provider shall provide to Client consulting services, requested modifications support services and other specialized support services with respect to the Technology and Services, at Service Provider's standard professional service fee rates then in effect. These services shall be provided by Service Provider remotely, but may be provided at Client location(s) if and when Service Provider and Client agree that on-site services are necessary.

e) Service Provider shall provide to Client modifications, revisions and updates in the Technology, Services, and Documentation, including changes Updates and Upgrades (as each are defined below) in programming languages, rules of operation and screen or report format, as and when they are implemented by Service Provider, provided such modifications, revisions or updates do not have a material adverse effect on the Technology as utilized by Client or the Services. "Update" means revisions or additions to the Technology which are intended to correct errors, improve efficiency or to incorporate additional or alternative functionality, but do not constitute substantial additional or alternative functionality, as customarily indicated by a change to the number to the right of the decimal in the version number, for example, Version 2.1 updated to Version 2.2. "Upgrade" means a new release of the Technology that incorporates substantial additional or alternative functionality, as customarily indicated by a change to the number to the left of the decimal in the version number, for example, Version 2.1 upgraded to Version 3.0. Updates and Upgrades will be made available to Client free of charge. With respect to Upgrades, however, Service Provider will provide notice to Client prior to installing an Upgrade for Client's benefit, and Client may decline or delay any such Upgrade in accordance with Client's business needs.

f) If an applicable Order includes the provision of certain implementation and training services with respect of the use of the Service, or assistance in creating Outputs (as defined below)) ("Implementation and Training Services"), then such services shall be provided in accordance with the SOW to be attached to the Order. The Implementation and Training Services shall be provided remotely (and not at Customer's site), unless otherwise agreed in writing between the Parties.

4. Use Restrictions.

a) Client shall not do, attempt to do, nor permit any affiliate or other person to do, any of the following: (i) create or recreate the source code for the Technology, or re-engineer, reverse engineer, decompile or disassemble the Technology; (ii) modify, adapt, translate or create derivative works based upon the Technology; (iii) remove, erase or tamper with any copyright or other proprietary notice printed or stamped on, affixed to, or encoded or recorded in any Technology; or (iv) sublicense, sell, lease, rent, timeshare or otherwise transfer, or pledge as security the Technology or its access to Service; (v) knowingly input, upload, transmit, or otherwise provide to or through the Services any information or materials that are unlawful or injurious; (vi) knowingly bypass or breach any security device or protection used by the Service, or knowingly submit any copyrighted material for which Client does not have rights through the Services. In the event that the Service Provider has a good faith belief that a violation of (v) and (vi) has occurred or is occurring, the Service Provider shall have the right, upon reasonable advanced written notice to the Client (if advance notice is feasible under the circumstance), to suspend the affected areas of Service until such violation is cured. Upon suspension contemplated in the immediately preceding sentence, the Parties should work in good faith to rectify the violation and restore the Service as quickly as reasonably practicable.

b) Service Provider shall perform all Services involving Client Confidential Information (including without limitation, PII and Client Data) in the United States, and in no event shall any Client Confidential Information be exported from or otherwise be accessed from outside of the United States without Client's express prior written permission. Out of an abundance of clarity, the Parties understand and agree that this restriction applies to any facilities Service Provider may be operating remotely. In addition, Service Provider shall not downgrade any security or data protection policies Service Provider utilizes as of the Effective Date of this Agreement or change the facilities from which it is providing the Services to Client without getting Client's prior written consent. Notwithstanding the foregoing, Client Confidential Information may be accessible by Service Provider's offshore affiliates located in Israel and Australia solely for the purpose of providing 24/7 support.

5. Proprietary Rights.

a) Service Provider, its affiliates and licensors, retain all right, title and interest in, to and under the Technology, Documentation, and Outputs. "Outputs" shall mean the interactive on-line guidance indicators deployed by the Services, to provide guidance and assistance to Users in acting and reacting (including by progressing through a process) within an applicable digital platform or application. Outputs exclude Client Confidential Information. Client acknowledges and agrees that the Technology, Services and Documentation, and components thereof, are subject to copyright, trade secret and other intellectual property protections in favor of Service Provider and its licensors. No title or right, or any intellectual property or other right, express or implied, is transferred to Client by virtue of this Agreement. The license granted hereunder is limited solely to the rights set forth herein. Client shall ensure that Service Provider's logos, patents, trademarks, service marks, copyrights, confidentiality and other notices or legends that are part of the Services, part of a download or report generated from Client's use of the Technology shall appear in their original and unaltered form on copies of all such downloads and reports.

b) The Parties understand and agree that all data contained in any Technology download or in any reports, spreadsheets or analysis of any kind generated by the Technology or via use of the Service, including all intellectual property rights therein and any enhancements, derivative works and improvements thereto ("Client Data") are the exclusive property of Client and nothing contained herein shall restrict Client

from using such Client Data in any way it deems fit. Service Provider shall only use Client Data for the benefit of Client as required to fulfill its obligations under this Agreement.

c) To the extent any development or customization work is performed by Service Provider related to this Agreement, then it shall be done pursuant to a separate Consulting Agreement negotiated between the parties.

6. Payment and Invoicing.

a) The fees due Service Provider for Services rendered and use of the Technology and Documentation set forth in an applicable Order and also referenced in the applicable Order Form ("Fees"), shall be invoiced upon the execution of such Order and shall due forty-five (45) days after Clients receipt of such invoice and excluding any amount that is the subject of a good faith dispute. Except as otherwise specified herein or in an Order: (i) the fees for the Services are based on the Service purchased and not on actual usage thereof, and fees paid are non-refundable; and (ii) Service ordered under an applicable Order Form and their respective payment obligations are non-cancelable.

b) All invoices shall be submitted to Client electronically in accordance with Client's electronic payment policies then in effect and provided to Service Provider in writing from time to time or made available for review at <http://www.comcast.com/vipgateway/?SCRedirect=true> and <https://account.rollstream.com/accounts/login> (the "Electronic Payment Policies"). Invoices shall be deemed received one business day after proper submission in accordance with the Electronic Payment Policies. Client reserves the right to reject any invoice that is not submitted in accordance with the Electronic Payment Policies.

7. Data Collection on Client Websites.

A) To the extent that any Services provided under this Agreement may include the placement of any pixels, scripts or code ("Code") on any website, mobile site or application or similar property or service of Client and such Code has the ability to include a function that collects data of an employee or a consultant of the Client regarding their browsing activity or provision of information by them to such a property or service or will be using any data collected from the internet in connection with providing any Services hereunder, Service Provider represents and warrants that it will not collect or use any such data without the express prior written permission of Client and then only in compliance with the restrictions set forth on Exhibit D hereto. Client reserves the right to scan Client's websites and applications for code provided by Supplier, and restrict and remove any code that is not in compliance with Client's Privacy Policy.

(B) Collection and Storage by WalkMe. For the purpose of providing the Service, the ongoing operation thereof, and/or for security purposes, WalkMe collects, processes and stores (i) End Users' IP addresses and country and city; (ii) e-mail addresses of Customer's personnel using the Service to create Outputs, or contacting WalkMe in connection with the provision of support. Such personal information would be collected, stored and processed only for Customer's benefit, and according to Customer's documented instructions and under Data Processing Agreement including any appendices thereto ("DPA") attached hereto. Additionally, if Customer avails itself of Supplier's analytics features, then additional user behavior data may be accessible by WalkMe. Such additional data is further described in Appendix 1a to the Data Processing

Addendum.

(C) Additional Undertakings. Customer shall be responsible for obtaining all consents and authorizations from End Users as may be required by any applicable law, for the collection, storage and processing of End User's information by WalkMe according to Customer's instructions and the DPA. WalkMe agrees that it shall comply with its obligations under the DPA in relation to the End User's information that WalkMe shall collect, process and stores as set out in section 7B above.

8. Confidential Information; Security; Access.

a) The Parties acknowledge and agree that they each may come into contact with confidential or proprietary information of the other Party, including but not limited to, vendor or supplier information, terms and conditions of supplier agreements, components or elements of the Technology, Services or Documentation, business plans and information, client and customer data, sales and product plans and data, PII, Usage Data, Client Data, all information about Client's network configuration, plant or any equipment attached thereto; and all other information relating to the software, operations, products or service offerings of Client which was disclosed or provided to Service Provider or became known to Service Provider through its relationship with Client or which a reasonable person knows or should know is confidential ("Confidential Information"). Notwithstanding anything in this Agreement to the contrary, the term "Confidential Information" shall not include any information that: (i) is or becomes generally known to the public other than as a result of a disclosure in breach of this Agreement; (ii) is rightfully in the possession of a Party prior to disclosure by the other Party; (iii) is received by a Party in good faith and without restriction from a third party having the right to make such disclosure and not under a confidentiality obligation to the other Party; or (iv) is independently developed by a Party without reference to the Confidential Information of the other Party, which such development may be demonstrated by documentation. The Parties acknowledge that the disclosure or unauthorized use of Confidential Information may cause irreparable injury and damages may not be readily ascertainable. The Parties shall, therefore, be entitled to seek injunctive relief upon a disclosure or improper use, or threatened disclosure or improper use, of any Confidential Information in addition to such other remedies as may be available at law or in equity.

b) "PII" means any information that refers, is related to, or is associated with an identified or identifiable individual, including, but not limited to, an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements: (i) Social Security number, (ii) driver's license number or state identification card number, (iii) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account or (iv) any individually identifiable information regarding an individual's medical history or medical treatment or diagnosis by a health care professional.

c) Non-use and Non-disclosure. The Parties shall, at all times, both during the Term of this Agreement and thereafter so long as such information continues to meet the definition of Confidential Information, use commercially reasonable efforts to keep all Confidential Information of the other Party confidential and shall only disclose the other Party's Confidential Information to those of its employees and permitted third parties as are necessary to fulfill such Party's obligations under this Agreement. The Parties each further agree that they will not, directly or indirectly, disclose any of the other Party's Confidential Information to any third party (except, with respect to Client, to its contractors and vendors that are performing services for Client) or use any of the other Party's Confidential Information for any purpose other than in furtherance of this Agreement except as specifically permitted by this Agreement or with the other Party's prior written

consent. Each Party will only allow those its employees and contractors to access the Confidential Information of the other Party that have a need to know in order to properly perform its obligations or exercise its rights under this Agreement and who are bound by the confidentiality provisions herein. Neither Party shall make any public statement relating to this Agreement without the other Party's prior written consent.

d) Service Provider hereby acknowledges that Client has a special responsibility under the law to keep PII private and confidential. Service Provider also acknowledges that the PII to which it may have access pursuant to this Agreement constitutes Client Confidential Information and that Service Provider in no way possesses or shall gain possession of any ownership or other proprietary rights with respect to such PII. Service Provider acknowledges and understands that PII is subject to the subscriber privacy protections set forth in Section 631 of the Cable Communications Policy Act of 1984, as amended (47 USC Sec. 551), as well as other applicable federal and state laws. Service Provider agrees that it shall (i) use such information in strict compliance with Section 631 and all other applicable laws governing the use, collection, disclosure and storage of such information; and (ii) ensure that its privacy policy is in accordance with applicable law, at all times during the term of this Agreement. Service Provider further agrees to restrict disclosure of such PII only for the purpose of provision of Services, to those Service Provider employees or sub-contractors with a need to know and who are bound by the confidentiality provisions herein and shall not further disclose such information to any third party without the prior written consent of Client, which may be withheld at its sole discretion. In the event that Client does provide such prior written consent in respect of a disclosure of PII to a third party, the Service Provider agrees that it shall, in accordance with the Law, provide the Client with all such information as may be required by the Client, upon reasonable request, to respond to requests from the Users.

e) Usage Data.

(i) Confidential Information shall include any and all usage data, activity data or other information collected from or about or otherwise regarding Client's users of the Services and/or Technology whether in individual or aggregate form ("Usage Data"). Such Usage Data is and shall remain the Confidential Information of Client. To the extent that Service Provider has access to or collects such Usage Data, it does so solely on behalf of Client pursuant to Service Provider's obligations hereunder and shall maintain the confidentiality of such data and shall treat in accordance with Client's then applicable privacy policies, privacy statements and applicable law. Service Provider shall not use Usage Data for any purpose not in compliance with its obligations under this Agreement and shall not disclose such data, whether in aggregate or individual form, to any third party. Notwithstanding the foregoing, either Party may disclose Confidential Information of the other Party if disclosure is required by a court of competent jurisdiction, but only after the Party seeking to disclose gives the other Party reasonable advance written notice to reasonably allow for an opportunity for such Party to secure an appropriate protective order or other measure limiting disclosure. The Parties shall reasonably cooperate in seeking such protection, at the expense of the Party seeking such protection.

(ii) The interconnected VoIP and telecommunications services provided to subscribers by Client are subject to the requirements of 47 U.S.C. § 222. In addition, the voice services provided to subscribers by Client are subject to the FCC's CPNI regulations, codified at 47 C.F.R. § 64.2001 et seq. To the extent Service Provider, its employees, agents, or subcontractors access, collect, process, and/or store the CPNI of Client subscribers while providing services to Client under this Agreement, Service Provider shall comply with 47 U.S.C. § 222 and any FCC regulations applicable to CPNI in the same manner and to the same extent as Client is obligated to comply as a provider of interconnected VoIP and telecommunications services as defined in 47 U.S.C. § 153(25) and (53), respectively. This includes compliance with the FCC's current CPNI regulations for voice services, 47 C.F.R. §§ 64.2001 – 64.2011, as well as any other regulations that may be adopted by the FCC during the term of this Agreement pursuant to 47 U.S.C. § 222.

Service Provider shall notify Client promptly, but in no case later than twenty-four hours following Service Provider's discovery of any actual or suspected unauthorized access, use, or disclosure of the CPNI of any Client subscriber, and shall take reasonable steps to remedy the breach and to prevent further unauthorized actions or other breach of this Agreement. Service Provider will cooperate with Client in every reasonable way in any subsequent investigations, regulatory actions, or litigation arising out of the breach. By executing this Agreement, Service Provider is representing that it will comply, and will ensure that its employees, agents, and subcontractors comply, with the requirements of 47 U.S.C. § 222 and all regulations applicable to CPNI, for the duration of this Agreement. This representation includes, but is not limited to, ensuring that all employees, agents, and subcontractors of Service Provider have been trained in the proper use, handling, and disclosure of CPNI prior to accessing the CPNI of any Client subscriber. For purposes of this Agreement, "**Customer Proprietary Network Information**" or "**CPNI**" has the meaning given to such term in 47 U.S.C. § 222(h)(1), 47 C.F.R. § 64.2003(g), and any other applicable rules that may be adopted by the Federal Communications Commission (FCC) during the term of this Agreement.

f) Security.

(i) All Client Confidential Information (including PII, CPNI and Usage Data) that is collected, stored or otherwise maintained by Service Provider pursuant to this Agreement shall be maintained in a secure environment that meets industry standards for website security and Client's IT security provisions set forth on Exhibit E (as such provisions may be updated in writing from time to time). Any Client Confidential Information (including PII and Usage Data) that is collected or obtained by Service Provider must be stored and transmitted in encrypted or otherwise secure form. In the event Service Provider engages in payment card transactions as a part of the services provided to Client, or services requiring access to or receipt and/or storage of information relating to credit card payment processing for Client's customers, Service Provider shall comply with the Payment Card Industry Data Security Standard ("PCI"), and any amendments or restatements of the PCI occurring during the term of this Agreement, and shall promptly implement all procedures and practices as may be necessary to remain in compliance with PCI, in each case, at Service Provider's sole cost and expense. Service Provider acknowledges that it is responsible for the security of customer credit card data in its possession. In connection with Service Provider's obligations under PCI, Service Provider agrees to cooperate with Client to determine and maintain records relating to the apportionment of responsibilities of Service Provider and Client under PCI Requirement 12.8.5. Service Provider will maintain and evidence PCI DSS compliance, and provide Client with a copy of Service Provider's "Report on Compliance" and "Attestation of Compliance" (as those terms are defined by the PCI Security Standards Council) promptly upon Client's request.

(ii) In the event that any periodic security audit conducted by Service Provider reveals a breach or a potential breach in Service Provider's security that may affect the security and/or integrity of Client Confidential Information, Service Provider will notify Client promptly and make all commercially reasonable efforts to re-secure its systems immediately, and if such is not possible then Service Provider shall shut the system down immediately until it can be re-secured.

(iii) In the event of an actual breach of security of any system, website, database, equipment or storage medium or facility controlled by Service Provider or a Service Provider contractor or vendor that results in a Security Breach, Service Provider shall notify Client promptly (but in no case longer than 24 hours following discovery of the issue), take immediate measures to prevent further unauthorized access, and shall cooperate with Client in the investigation and remediation of any such occurrence, including any actions that may be required by any applicable Card Network. Such remediation may include, but is not limited to, (i) the provision of notice concerning such occurrence to any person affected or potentially affected thereby and applicable domestic and international authorities, and (ii) with respect to any Security Breach that poses a risk of identity theft, including but not limited to a Security Breach involving a Social

Security number, driver's license number or similar personal identification number, the provision of daily credit monitoring, access to credit reports and identity theft insurance to any person affected or potentially affected thereby. To the extent that a Security Breach results from Service Provider's failure to comply with its representations, warranties and/or obligations hereunder, Service Provider shall reimburse Client for remediation costs incurred by Client in connection with such Security Breach.

(iv) For purposes of this Agreement, (A) "Security Breach" means (i) any breach of security of any system, website, database, equipment or storage medium or facility controlled by Service Provider or a service provider contractor or vendor of Service Provider that results in unauthorized access to Client Confidential Information (including PII and Usage Data) by any third party (including any employee or subcontractor of Service Provider that is not authorized to access such information), or any loss, misuse, destruction, deletion or modification of Client Confidential Information (including PII and Usage Data) or that may compromise Client's internal business network; or (ii) any act or omission of Service Provider (including any subcontractors) or any third party that compromises the security, confidentiality, or integrity of Client Confidential Information (including PII and Usage Data) or Client's internal business network, or the physical, technical administrative or organizational safeguards put in place by Service Provider (or its subcontractors) that relate to the protection of the security, confidentiality or integrity of the Client Confidential Information (including PII and Usage Data) or Client's internal business network and (B) "Card Network" means Visa USA, Inc., MasterCard International, American Express and Discover Card.

g) Adequacy of Employees and Sub-contractors.

(i) Service Provider shall cause a Background Check (as defined below) to be completed on all Personnel (including, for avoidance of doubt, any personnel of subcontractors used by Service Provider) assigned by Service Provider to provide Services hereunder prior to the date such Services commence and shall not assign Personnel to provide Services hereunder if the results of any Background Check, or Service Provider's actual knowledge, indicate that such Personnel may pose a threat to Client's property, employees, subscribers, subscribers' property or Confidential Information or such Personnel would be otherwise unsuitable for assignment.

(ii) For purposes of this Section 8(g), a "Background Check" means a background investigation performed by an agency in good standing with the National Association of Professional Background Screeners, and shall include, but not be limited to, (1) a check of felony and misdemeanor criminal convictions (federal, state and county) for at least the immediately preceding seven (7) year period, (2) searches of the U.S. Government Specially Designated National (OFAC) and export denial lists and relevant national and state sex offender registries, and (3) verification of the individual's citizenship and legal right to work in the jurisdiction in which the Personnel would be performing the Services. For any period of time encompassed in the foregoing background check requirement when an individual was resident outside of the United States, such background checking shall be conducted by a reputable investigative agency that conducts background checking in the relevant country(ies), utilizing database checking, field checking and interviews as needed.

(iii) Service Provider shall comply with all applicable laws in conducting the background check specified in this Section 8(g) including but not limited to securing from each individual who provides Services for Client written consent to perform the background checking specified in this Section 8(g) and provide reasonably sufficient proof of the completion of such background checks upon request. Care should be taken by Service Provider to ensure that all assignment decisions are in accordance with applicable state and federal regulations regarding hiring practices. Service Provider should consult with its local human resources expert and/or legal counsel to ensure compliance with such guidelines and applicable law.

(iv) The Parties understand and agree that the nature of the information that Service Provider Personnel may access, as well as the requirements of applicable law, may change from time-to-time, and in such cases, upon the request of Client the Parties will work together in good faith to modify this Section 8(g) and/or the applicable Statement of Work to address any such changes.

(v) Service Provider shall indemnify, defend and hold Client harmless from any allegation, claim, suit, action or proceeding (each an "Action") against Client or any of its affiliates, officers, directors, members, employees, contractors and/or agents, arising from any violation of this Section 8(g) by Service Provider or its subcontractors. Failure of Service Provider or its subcontractors to comply with this Section 8(g) shall constitute a material breach of this Agreement and entitle Client to terminate the Agreement upon provision of written notice to Service Provider. At all times while performing Services, Service Provider Personnel shall not (1) possess, distribute, manufacture or use any illicit drug; (2) consume or possess alcohol; (3) possess any prescription drug for any person other than the person for whom the drug is prescribed or abuse any prescribed drug; or (4) perform Services under the influence of alcohol and/or illicit drugs. If Client, in good faith and for non-discriminatory and non-arbitrary reasons, does not wish for an individual to perform or continue performing Services, then Client will so notify Service Provider in writing or via email, and said writing or email shall include as much specific information about Client's material concerns as Client determines is reasonable under the circumstances. In response to said notice, Service Provider agrees that it will not thereafter permit said individual to perform Services for Client.

(vi) Notwithstanding any provision to the contrary and for purposes of clarity, the Parties understand and agree that Service Provider Personnel will be (1) the employees or subcontractors of Service Provider only, and Service Provider alone will determine the terms and conditions of such employment or engagement; and (2) hired, paid, supervised, directed, controlled, promoted or demoted, terminated, engaged and otherwise managed solely by Service Provider.

h) Remote Access. To the extent that Client allows Service Provider to gain remote access to Client's networks or equipment for purposes of performing its obligations hereunder, Service Provider shall ensure that (i) such access is restricted to authorized employees; (ii) it provides Client with a list of all such authorized employees, who shall undergo and pass a then recent criminal background check; (iii) such remote access is used solely for purposes of fulfilling Service Provider's obligations under this Agreement; (iv) such remote access is obtained through a secure connection; (v) Service Provider and all Service Provider Personnel comply with Client's IT security provisions set forth on Exhibit E (as such provisions may be updated in writing from time to time) and (vi) Service Provider uses such remote access capability only to access equipment or software that is directly involved in Service Provider's performance of its obligations hereunder and does not access any other Client, Client Affiliate or third party systems, databases, equipment or software. Upon Client's request, Service Provider will provide periodic security audits of its access system and methods and will change authentication elements periodically to maintain the integrity and security of Service Provider's access.

i) Facility Access. Service Provider agrees that it and its employees and subcontractors who gain access to Client's or any of its affiliate's in connection with the performance of this Agreement will at all times comply with Client's safety and security policies, visitor guidelines and all other applicable policies. Service Provider and such employees and subcontractors who access Client's or any of its affiliate's premises shall have passed a then recent criminal background check and shall access only those areas expressly permitted by Client and shall not attempt to access any other facilities or portions thereof without Client's prior express approval. Service Provider shall be responsible for the actions of its employees and subcontractors.

j) Comcast may share the Agreement (including all of its terms and conditions and all Annexes, Exhibits, attachments, and all Orders, SOWs and purchase orders hereunder) with any of its current and future

Affiliates so that such Affiliate can make a determination regarding the Agreement for its business needs, so long as such Affiliate is subject to or agrees to be subject to confidentiality obligations substantively similar to the terms contained herein.

k) The Parties acknowledge and agree that upon termination of this Agreement, or at any time upon written request, either Party or both Parties shall promptly return or destroy all memoranda, notes, records, reports, media and other documents and materials (and all copies thereof) in that Party's possession, custody or control regarding or including any Confidential Information of the other Party.

l) Pursuant to jurisdictional requirements specific to India, China, Australia, Singapore, the European Union and California, Exhibit H-1, titled Data Processing Addendum For Access and Services Agreement, and H-2 titled "Limitation on Use of Personal Information; Consumer Requests is incorporated into this Agreement by reference herein.

9. Publicity and Press Release. Except as required by law, neither Party shall disclose, advertise, or publish the terms and conditions of this Agreement or the fact this Agreement exists without the prior written consent of the other Party.

10. Limited Warranty.

a) Service Provider represents and warrants that:

- (i) it is not bound by any agreements, obligations or restrictions and will not assume any obligation or restriction or enter into any other agreement that would interfere with its obligations under this Agreement, and to Service Provider's knowledge as of the Effective Date, it's entering into the Agreement, granting the licenses set forth herein or the performance of any Services and obligations hereunder do not violate any applicable law or right of any third party;
- (ii) it (and the employees or subcontractors furnished or utilized by Service Provider hereunder) possess the knowledge, skill and experience necessary to perform the Services required hereunder;
- (iii) prior to making any Technology or Service available to Client under this Agreement, Service Provider will use commercially available virus checking software to scan such Technology or for malicious components (e.g., computer virus, worm, time bomb, or otherwise) that could, in any material way, damage any software, firmware or hardware of Client, and remove any such identified components;
- (iv) during the Term, the Technology will perform and the Services associated with the Technology will be provided in all material respects in accordance with its Documentation and the description set forth on Exhibit A (if any). Client's remedy and Service Provider's obligation for any such failure will be for Service Provider to use its commercially reasonable efforts to correct such non-compliance; provided however that if Service Provider fails to remedy such non-compliance in all material ways within a commercially reasonable time, and after a reasonable number of attempts, Service Provider shall, upon Client's written request, provide to Client a pro-rata refund of any pre-paid, unused Fees for the applicable Services;
- (v) neither the Technology nor Client's use of or access to the Technology will subject Client or any of its software to any Excluded License. An "Excluded License" is any license that requires as a condition of use, modification and/or distribution of software subject to such license, that such software or other software combined and/or distributed with such software be

(1) disclosed or distributed in source code form; (2) licensed for the purpose of making derivative works; or (3) redistributable at no charge;

(vi) during the Term, it will perform the Services in a workmanlike manner consistent with generally accepted industry standards, and that for a period of thirty (30) days from acceptance of any Services performed pursuant to an SOW that involve Deliverables, the Deliverables will perform in all material respects in accordance with any applicable specifications set forth in (or attached to) the applicable SOW. In the event of a breach of the foregoing warranty, Service Provider shall re-perform the applicable Services free of charge; provided however that if Service Provider re-performs such Services and the new Deliverable continues to fail to perform in accordance with the applicable specification, Service Provider shall, upon Client's written request, provide to Client a pro-rata refund of all fees paid pursuant to the SOW and shall not owe any further fees pursuant to such SOW; and

(vii) it (and the employees or subcontractors furnished or utilized by Service Provider hereunder) shall comply with all applicable laws, rules, regulations and self-regulatory codes relating to its performance hereunder.

b) EXCEPT AS SPECIFICALLY SET FORTH HEREIN, SERVICE PROVIDER AND ITS LICENSORS MAKE NO WARRANTIES AS TO THE TECHNOLOGY, SERVICES AND DOCUMENTATION AND EACH EXPRESSLY DISCLAIMS ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF FITNESS FOR PARTICULAR PURPOSE, MERCHANTABILITY, TITLE OR NON-INFRINGEMENT OR THAT THE SERVICES WILL BE FREE OF ERROR. NO ACT OR STATEMENT BY SERVICE PROVIDER OR ITS PERSONNEL SHALL OPERATE TO MAKE OR CONSTITUTE A WARRANTY OR REPRESENTATION.

11. Indemnification from Third Party Claims. Service Provider agrees to defend, indemnify and hold harmless Client, its affiliates, and each of their employees, directors and consultants (each a "Client Indemnitee"), from and against any third party claim or action: (a) based on Service Provider's breach of its obligations, covenants or warranties as set forth in this Agreement under Section 7 (Data Collection on Client Websites), Section 8 (Confidential Information; Security; Access), Section 9 (Publicity and Press Release), and under subsections 10 (a) (i), (iii), (v), (vii) and Section 17 (Miscellaneous) under subsections (m), (n), and (o); or (b) that the Technology, Services (including any metadata associated with the Service), Deliverables or Documentation (each whether alone or as an essential part of a combination) infringes a patent, copyright, trade secret, trade mark or any other intellectual property right of a third party. Pursuant to the foregoing Service Provider shall only be liable for amounts awarded by a court of competent jurisdiction, in arbitration, or in settlement. The foregoing is expressly conditioned upon: (i) Service Provider being promptly notified in writing of such claim; (ii) Client Indemnitee granting Service Provider sole control of the defense and any related settlement negotiations, provided that Service Provider may not enter into any settlement agreement that obligates Client Indemnitee or attributes liability to Client Indemnitee without Client Indemnitee's prior written consent; and (iii) Client Indemnitee reasonably cooperates with Service Provider (at Service Providers expense) in the defense of such claim. If the Client's permitted access to or use of the Technology, Service or any Deliverables is or may be enjoined due to an intellectual property claim, Service Provider will use commercially reasonable efforts to either modify or replace the allegedly infringing part of the Technology, Service or Deliverable with a non-infringing version of no less than materially equivalent functionality or obtain a license permitting Client's continued use of or access to the allegedly infringing part of the Technology, Service or Deliverable. If after using commercially reasonable efforts, Service Provider does not or cannot provide either of these options, and the Client's use of or access to the Technology, Service or Deliverable, as applicable, is adversely affected, then Client may immediately terminate this Agreement upon written notice to Service Provider and Service Provider shall refund to Client a pro rata portion of any prepaid Fees from the

effective date of termination through the last day of the period for which the Fees were prepaid. In no event will WalkMe have any obligation or liability under this Section 11 arising solely from: (i) use of any Service in a modified form, unless WalkMe performed or authorized in writing such modification; (ii) combination of the Services with materials not furnished by WalkMe, unless (A) WalkMe sold, made, recommended, or approved the Service for combination with such materials, or (B) the combination would be commercially reasonably contemplated for the intended use of the Services as provided under this Agreement; and (ii) any failure by Client to comply with the use restrictions of Section 4(a) of this Agreement. The foregoing states the entire liability of Service Provider with respect to claims of infringement of any patents, copyrights, service marks, trade secrets, trademarks or any other intellectual property right of a third party by the Technology, Services, Documentation or Deliverables or any part thereof.

12. Limitation of Liability.

a) EXCEPT FOR SERVICE PROVIDER'S INDEMNIFICATION OBLIGATIONS SET FORTH IN SECTION 11, CLIENT'S BREACH OF SECTION 4(A), A PARTY'S BREACH OF SECTION 8, A PARTY'S ACTIONS THAT CAUSE PERSONAL INJURY OR THAT ARE CATEGORIZED AS GROSS NEGLIGENCE OR INTENTIONAL MISCONDUCT, IN NO EVENT SHALL CLIENT OR SERVICE PROVIDER, THEIR AFFILIATES, SUPPLIERS OR LICENSORS, BE LIABLE FOR COSTS OF PROCUREMENT OR SUBSTITUTE SERVICES OR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING BUT NOT LIMITED TO, DAMAGES RESULTING FROM LOSS OF PROFITS, DATA, USE OF DATA OR LOSS OF BUSINESS ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, EVEN IF AWARE OF THE POSSIBILITY OF SUCH DAMAGES.

b) EXCEPT FOR SERVICE PROVIDER'S INDEMNIFICATION OBLIGATIONS SET FORTH IN SECTION 11, CLIENT'S BREACH OF SECTION 4(A), A PARTY'S BREACH OF SECTION 8, A PARTY'S ACTIONS THAT CAUSE PERSONAL INJURY OR THAT ARE CATEGORIZED AS GROSS NEGLIGENCE OR INTENTIONAL MISCONDUCT, THE AGGREGATE LIABILITY OF EITHER PARTY, OR ITS AFFILIATES, SUPPLIERS OR LICENSORS, FOR DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, SHALL NOT EXCEED THE GREATER OF THE FEES PAID TO SERVICE PROVIDER HEREUNDER WITHIN THE LAST TWELVE MONTH PERIOD, OR \$5,000,000, WITHOUT REGARD TO WHETHER A CLAIM IS BASED ON CONTRACT OR TORT, INCLUDING NEGLIGENCE.

13. Term; Termination.

a) This Agreement shall remain in effect for an initial term of three (3) years ("Initial Term"), beginning on the Effective Date and shall automatically renew for successive one year terms ("Renewal Term") (the Initial Term and any Renewal Term shall be collectively referred to herein as the "Term") unless and until either Party gives notice of intent not to renew at least ninety (90) days in advance of the end of the then current term.

b) [Intentionally omitted]

c) Either Party may terminate this Agreement or Order for cause of if the other Party commits a material breach of this Agreement that remains uncured after the expiration of thirty (30) days' written notice

specifying the basis for the breach. Termination of one Order under this Agreement shall not be deemed a termination of another Order.

d) Either Party may terminate this Agreement immediately if the other Party (i) becomes insolvent or makes a general assignment for the benefit of creditors; (ii) suffers or permits the appointment of a conservator or receiver for its business or assets or any similar action by a governmental entity for the purpose of assuming operation or control of the Party due to the financial condition of the Party; (iii) becomes subject to any proceeding under any bankruptcy or insolvency law whether domestic or foreign, and such proceeding or action has not been dismissed within a sixty (60) day period; or (iv) has wound up or liquidated its business, voluntarily or otherwise.

e) Upon any notice of such termination, Service Provider shall provide Client (at Client's request) the "Termination Assistance" described in Exhibit F (such period of time where Service Provider provides Client with Termination Assistance shall be referred to herein as the "Termination Assistance Period"). If Service Provider provides Client with termination Assistance, the Agreement shall be considered terminated at the end of such Termination Assistance Period.

f) Upon termination of this Agreement, User's Access to the Technology shall immediately terminate. Anything to the contrary herein notwithstanding, immediately upon the termination of this Agreement: (i) Service Provider shall transfer to Client any data in process with Service Provider at that time and any Client Confidential Information, including all related documentation and copies thereof, in Service Provider's possession; and (ii) Client shall return or destroy the Documentation and any Service Provider Confidential Information in Client's possession.

14. Audit. Each Party shall maintain accurate records of all material expenses, revenues, fees, transactions and related documentation (including agreements) in connection with the performance of the Agreement (the "**Records**"). All such Records that are financial in nature shall be maintained in accordance with generally accepted accounting practices during the Term, and for six (6) months following termination of the Agreement. For the sole purpose of ensuring compliance with this Agreement, each Party shall have the right during the Term and for six (6) months after the expiration or termination of this Agreement, at its expense and upon terms that are mutually and reasonably agreeable to both Parties, to conduct a reasonable inspection of portions of the Records of the other Party that are directly related to amounts payable to the Party requesting the audit, pursuant to the Agreement. Any such audit may be conducted after forty-five (45) days prior written notice, subject to the following: Such audits shall not take place more frequently than once every twelve months and provided that prior to entering a Party's premises, the Party seeking the audit (and all third party consultants accompanying such Party) agree to be bound a confidentiality agreement protecting the audited Party's confidential information and to the security, safety and privacy policies in place at the site.

15. Insurance.

a) During the Term and, with respect to policies maintained on a claims-made basis, for a period of three years thereafter, Service Provider will obtain and keep in force not less than the following Insurance:

(i) Commercial General Liability insurance, including bodily injury, property damage, and personal & advertising injury with limits of not less than \$1,000,000 combined single limit per occurrence and \$2,000,000 annual aggregate, naming Client and each of its officers, directors and employees as additional insureds;

(ii) Workers' Compensation as provided for in any jurisdiction where work is performed by Service Provider Personnel who are engaged in the performance of Services under this Agreement with an Employer's Liability limit of not less than \$1,000,000 for bodily injury by accident or disease;

(iii) Business Auto insurance covering non-owned and hired autos with limit of not less than \$500,000 combined single limit per accident for bodily injury and property damage liability, naming Client, its officers, directors, and employees as additional insureds;

(iv) Umbrella/Excess Liability with limits of not less than \$4,000,000 combined single limit in excess of the above-referenced Commercial General Liability, Employer's Liability and Business Auto Liability;

(v) Technology Errors and Omissions Liability. Covering the liability for financial loss due to error, omission, negligence of employees and machine malfunction, and including coverage for introduction of a computer virus onto, allowing unauthorized access to, denial of service, or otherwise causing damage to, a computer, computer system, network, or similar computer-related property and the data, software and programs used thereon, as well as cyber liability and privacy, in an amount of at least Five Million Dollars (\$5,000,000) per occurrence. Coverage will include intentional or unintentional disclosure of private personal or corporate information. Liability will also include the cost of regulatory action defense and fines/penalties, privacy breach notification, fraud monitoring, and public relations expenses, whether computer-related or not. These amounts will not be sublimited, nor will costs be limited to those mandated by statute or regulation; and

(vi) Crime Insurance (also known as Employee Dishonesty insurance/ Fidelity Bond). In an amount of not less than One Million Dollars (\$1,000,000) per occurrence covering all Service Provider Personnel and including coverage for cybercrime and privacy breaches and a Client's Property endorsement or Insuring Agreement specifying that Employee Theft coverage extends to Client's property in the event of any theft of Client's money or property, or money or property of other persons for which Client is responsible. Verification that Client has been included as a Joint Loss payee under the policy must be provided.

b) All required insurance policies must be taken out with financially reputable insurers rated A-, VII or better or otherwise reasonably acceptable to Client and licensed to do business in all jurisdictions where Services are provided under this Agreement. Service Provider will provide Client, upon request, with a certificate of insurance, on a current ACORD form or an equivalent form satisfactory in form and content to Client, evidencing that all the required coverages are in force and have been endorsed to provide that no policy will be cancelled or materially altered without first giving Client at least thirty (30) days' prior notice.

c) The foregoing insurance coverage shall be primary and non-contributing with respect to any other insurance or self-insurance which may be maintained by Client. Each such insurance policy carried by Service Provider shall grant waiver of subrogation in favour of Client and its parents, subsidiaries, and affiliated companies. Service Provider shall ensure that its subcontractors, if any, maintain reasonably adequate insurance coverage.

16. Back-Up; Disaster Recover; Business Availability. During the Term, Service Provider shall: (i) back-up the files containing Client Data as well as all active Service Provider data bases to two (2) geographically separate data centers, and (ii) maintain a commercially reasonable Disaster Recovery and Business Continuity Plan (as defined below). The "Disaster Recovery and Business Continuity Plan" is a plan that allows for the continued provision of Services to Client, in accordance with the service level criteria set forth in Exhibit B, in the event of an emergency that provides for and documents (a) data, system and network recovery procedures, (b) data, system, and network connectivity fail-over procedures, and (c) how Service Provider will interact with its disaster recovery team. Service Provider shall test the Business Continuity Plan as least once a year.

17. Miscellaneous.

a) The Parties agree that the relationship between them is solely that of independent contractors, not employment, partner, joint venture, funds or money transmitter, payment clearinghouse, or agent, and that no act or statement of either of them will operate to bind the other and that neither Party shall hold itself out or have any authority as an agent of the other for any purpose whatsoever. No provision of this Agreement shall be interpreted to make the relationship of the Parties hereto exclusive to each other. Each Party is free to contract with other parties with respect to the services provided hereunder.

b) The Fees specified herein do not include applicable transaction taxes. If Service Provider is required to pay any federal, state, county, local or value added tax (VAT), sales and use tax, goods and services tax (GST) or similar applicable taxes by law, based on the Services provided, Service Provider shall ensure that Fees are invoiced to Client in accordance with applicable rules so as to allow Client to reclaim such value-added and/or similar tax from the appropriate government authority. Nothing in this Agreement, however, shall require Client to pay any payroll, franchise, corporate, partnership, succession, transfer, income, excise, profits or income tax of Service Provider. If Client is required by government regulation to withhold taxes for which Service Provider is responsible, Client shall deduct such withholding tax from payment to Service Provider and provide to Service Provider a valid tax receipt in Service Provider's name. If Service Provider is exempt from such withholding taxes as a result of a tax treaty or other regime, Service Provider shall provide to Client a valid tax treaty residency certificate or other tax exemption certificate at a minimum of thirty (30) days prior to payment being due. Should either Party realize that any tax included or omitted as a result of the transactions hereunder was made in error, the Parties shall cooperate to resolve such overpayment or underpayment and to further assist in refunding or charging of any mistaken payments.

c) Comcast Affiliates may either (i) make use of an Order or SOW signed by Comcast Cable Communications Management, LLC, in which case Comcast Cable Communications Management, LLC will be responsible for such Affiliate's compliance with the terms and conditions hereof and any Order or SOW, including payment obligations, or (ii) execute an independent Order or SOW hereunder, in which case such Affiliate will, for purposes of such Order, be deemed "Client" for all purposes of the Order or SOW. Any Order or SOW between a Client Affiliate and Service Provider shall constitute a separate and independent agreement between the Client Affiliate and Service Provider, the Client Affiliate will be solely responsible and liable for its own compliance with the terms of this Agreement and such Order, including payment obligations, and actions pursuant to such agreement shall not affect the validity of this Agreement or any other Order or SOW between Client and Service Provider. In addition, a Comcast Affiliate that desires to execute an independent Order or SOW hereunder may further execute a Joinder Notice, in the form set forth on Exhibit G and as mutually agreed by such Comcast Affiliate and the Service Provider, which shall create a single relationship between Service Provider and the signing Affiliate whereby the obligations and liabilities set forth in the Agreement, as well as any additional terms and conditions mutually agreed to by the Parties in the Joinder Notice, run between Service Provider and the signing Affiliate only.

d) All the terms, provisions and conditions of this Agreement shall be binding upon and inure to the Parties hereto and their respective permitted successors and assigns. Service Provider shall not assign this Agreement without Client's prior written consent except to successor in interest related to a merger or acquisition provided that Service Provider uses commercially reasonable efforts to provide notice to the Client prior to any assignment. In the event that Service Provider cannot provide prior notice the Service Provider shall give Client notice at time such assignment and Client may terminate the Agreement and any Services, without penalty, upon written notice to Service Provider. Client may assign this Agreement upon notice to Service Provider. In the event of termination pursuant to this paragraph of this Agreement and any Services by Client, Service Provider shall refund to Client a pro rata portion of any prepaid Fees from the effective date of termination through the last day of the period for which the Fees were prepaid. Subject to the foregoing, this Agreement shall be binding upon and insure to the benefit of the parties hereto, their successors and permitted assigns. This Agreement is solely for the benefit of the Parties, their permitted

successors and assigns and shall not, unless expressly set forth herein, confer any rights or remedies on any third party.

e) The provisions of this Agreement which by their nature are intended to continue beyond the termination of this Agreement or the completion of any services, including, but not limited to, Sections 1, 4, 5, 7 - 9, 11 - 15 and 17 shall survive the expiration or the termination of this Agreement by any Party for any reason.

f) Client is committed to providing equal access and meaningful opportunities to all vendors. Our supplier diversity program is designed to maximize the inclusion of the following: Minority Business Enterprise; Women Business Enterprise; Veteran Business Enterprise; Service Disabled Veteran Business Enterprise; Historically Underutilized Business Enterprise; Lesbian, Gay, Bisexual, Transgender Business Enterprise; Persons with Disabilities; and Small Business (collectively, "Diverse Suppliers") in our supply chain. Client encourages our vendors to explore all available opportunities to partner with Diverse Suppliers who offer complementary products and/or services to be provided under any agreement. Client expects any such arrangements to augment and not duplicate, the responsibilities and efforts of the Service Provider and other suppliers engaged in the provision of the Services and/or Technology contemplated under this Agreement. We reserve the right to periodically evaluate Service Provider's supplier diversity performance as an important consideration in the award of additional business opportunities with Client.

g) Notices. All communications, notices, and exchanges of information contemplated in this Agreement or required to be given by this Agreement shall be in writing and shall be deemed to be properly given when personally delivered to the person identified in the notice section of the signature page, two (2) days after a Party deposits same in first class U.S. mail, postage prepaid, addressed to the other Party at the address set forth on the signature page of this Agreement.

h) This Agreement may not be changed, modified or rescinded except in writing, signed by the Party against whom enforcement is sought, and any attempt at oral modification of this Agreement shall be void and of no effect. If any provision of this Agreement is declared void or unenforceable, such provision shall be subject to reformation to best express the Parties' original intent or, failing that, deemed severed from this Agreement, and the remaining provisions of this Agreement shall otherwise remain in full force and effect.

i) This Agreement and its interpretation shall be governed by the internal laws of the State of New York, without giving effect to the conflict of laws or choice of law provisions thereof. The Parties agree that all suits brought with respect to the terms and conditions of this Agreement shall be exclusively filed in the state and federal courts of the State of New York and each Party hereby waives all forum non conveniens and personal jurisdiction arguments or defenses it may have with respect to any such action.

j) This Agreement, including all exhibits, attachments, Orders, statements of work or work orders, constitutes the entire agreement between the Parties and their respective Affiliates with respect to the subject matter hereof and supersedes all prior agreements and understandings, both oral and written, between the Parties and their respective Affiliates. In the event of a conflict between the terms and conditions in this Agreement and any Orders, SOWs or work orders or attachments hereunder, the terms and conditions of this Agreement shall control, except to the extent that specific language in an Order, SOW or work order executed by both Parties expressly states that it supersedes particular language in this Agreement or as incorporated via a written amendment executed by both Parties. This Agreement and any Order, SOW or work order issued hereunder shall prevail over any terms stipulated on any purchase order. Additional or conflicting terms contained in any Client or Service Provider purchase order, standardized form or correspondence are expressly unenforceable under this Agreement unless such terms and conditions

are contained in an amendment to this Agreement or the applicable Order, SOW or work order duly executed by both Parties.

k) No failure or delay by either Party in exercising any right under this Agreement shall operate as a waiver of such right.

l) Neither Party shall be liable to the other Party for failing to perform its obligations hereunder because of circumstances beyond the reasonable control of the non-performing Party for so long as such circumstances continue despite the commercially reasonable efforts of the non-performing Party to remedy the situation or provide a suitable workaround. Such circumstances shall include, but not be limited to, a natural disaster, act of a public enemy, acts of terrorism, riot, sabotage, strikes, power failure, acts of God, third party communication system problems, or any other such events beyond the reasonable control of non-performing Party.

m) Equal Opportunity Employer. Client is an equal opportunity employer and is a federal contractor. Consequently, the Parties agree that, to the extent applicable, they will comply with Executive Order 11246, The Vietnam Era Veterans Readjustment Assistant Act of 1974 and Section 503 of the Vocational Rehabilitation Act of 1973 and also agree that these laws are incorporated herein by reference.

n) Federal Contractor Requirements. **Client and Service Provider shall abide by the requirements of 41 CFR §§ 60-1.4(a), 60-300.5(a) and 60-741.5(a). These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities, and prohibit discrimination against all individuals based on their race, color, religion, gender identity, sexual orientation, sex, or national origin. Moreover, these regulations require that covered prime contractors and subcontractors take affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, national origin, protected veteran status or disability. The Parties also agree that, as applicable, they will abide by the requirements of Executive Order 13496 (29 CFR Part 471, Appendix A to Subpart A), relating to the notice of employee rights under federal labor laws.**

o) Local Wage and Benefit Ordinances and Standards. In certain jurisdictions, Client may be required to comply with local wage and benefit ordinances and standards ("Standards"), which typically require employers to pay employees wages at a rate that exceeds the minimum wage levels established by state and federal law and/or to provide a certain level of benefits. As a result of this Agreement, Service Provider also may be required to comply with applicable Standards. Consequently, the Service Provider agrees that it will take all necessary steps to ensure it understands the scope of all applicable Standards, including consultation with its local human resources professionals and/or legal counsel, and, to the extent it is covered or workers provided to Client are covered, to ensure compliance with all such Standards.


p) Counterparts; Execution. This Agreement and each attachment including an Order or SOW may be executed in multiple counterparts, each of which shall be deemed an original and all of which when taken together shall constitute one and the same instrument. Electronically transmitted or electronically executed signatures (including via facsimile or electronically scanned transmission) shall have the full force and effect of an original signature. The Parties consent to the use of a third party service for purposes of electronically signing the Agreement and agree to be bound by electronic signature.

q) Subcontractors. Service Provider shall not subcontract the Services under this Agreement, to any third party without (i) the prior written consent of Client, which may be withheld at its sole discretion, and (ii) the prior written agreement of the proposed subcontractor to be bound by the provisions of this Agreement. Notwithstanding any such subcontract, Service Provider shall not be relieved of its performance or obligations under this Agreement. Service Provider shall be solely responsible for each subcontractor's

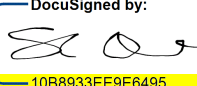
full and timely performance, and the acts and omissions of each subcontractor shall be deemed and treated as the acts and omissions of Service Provider itself. Service Provider shall also be solely responsible for compensating any subcontractor. Client agrees that Exhibit I contains a list of approved subcontractors under this Agreement.

IN WITNESS WHEREOF, each of the Parties has caused this Agreement to be executed by its duly authorized representative.

COMCAST CABLE COMMUNICATIONS
MANAGEMENT, LLC

By: 
46C3A4E1D797462...
Name: Leslie Fein
Title: SVP Procurement
Date: 09/30/2020

WALKME, INC.

DocuSigned by:

10B8933EE9E6495...
By: Shane Orlick
Name: CRO
Title: 9/29/2020
Date:

Address for Notices:

For Client:

Comcast Cable Communications Management, LLC
One Comcast Center
1701 JFK Boulevard
Philadelphia, PA 19103-2838
Attention: VP, Strategic Procurement

With a copy to:
Comcast Cable Communications Management, LLC
One Comcast Center, 50th Floor
1701 JFK Boulevard
Philadelphia, PA 19103-2838
Attention: General Counsel, Comcast Cable

For WalkMe:

71 Stevenson Street, 20th Floor
San Francisco, CA 94105
Attn: Legal Department

Exhibit A**DESCRIPTION OF SERVICES AND TECHNOLOGY**

(The following is a general overview of WalkMe's product and services. The subscription purchased in the Order Form may include the following:

Modules	Features & Description
----------------	-----------------------------------

Web (System)	
WalkMe Player™	The WalkMe Player is responsible for playing WalkMe-generated content for the End User. The WalkMe Player is also used as the central repository for all training material Customer wants to put at its End Users' fingertips for all applications Customer enables with WalkMe. Analytics are collected for all End User interaction with all types of content accessed through the WalkMe Player, whether it was generated via the WalkMe Editor, or imported into the repository from external sources.
WalkMe Editor™	The WalkMe Editor is a content editor and management console used to design and configure unlimited amounts and varieties of WalkMe content, including:
Applications	Walk-Thrus, Launchers, Resources, Search, Onboarding, Shuttles, Surveys and ShoutOuts.
Integration Modules	Integrate WalkMe applications with Customer and/or third party applications such as Search, Help Desk, Chat and Salesforce.com Enhanced Search
User ExperienceControl	Control and enhance user experience. Customize the look and feel of the WalkMe Player and balloons. Make the WalkMe experience stand out, or let it blend right into your application.
Access Control	Roles and user management. Assign roles to users (sub-accounts) that will have access to the WalkMe Editor, who can publish new content, and will have access to the analytics.
WalkMe Insights™	WalkMe Insights provides Customers with advanced BI and dashboard capabilities. Customers leverage the analytics tools to better understand End User performance and gain important insights into End User adoption, measuring goals completion, engagement/stickiness of your application(s) and wide range of other important metrics. To get insights and track goals.
API	Directly access WalkMe functionality (i.e. opening the WalkMe menu, or starting a Walk-Thru) via API call. Also provides direct access to information about the current state of WalkMe on a website.
Mobile	
WalkMe MobileSDK™	The WalkMe Mobile SDK is responsible for managing all the mobile campaigns in real time within the Customer application. The WalkMe Mobile SDK is equipped with technology that collects hundreds of parameters each session. The WalkMe Mobile SDK manages and analyzes the data and increases performance results in real time.
WalkMe In-App Editor™	The WalkMe In-App Editor is a content editor and management console used to design and configure unlimited amounts and varieties of WalkMe content, including:
Applications	Using the drag and drop editor, create and launch in-app messages and walkthroughs directly to the company app. campaigns created within the WalkMe In-App Editor will be translated in to native code for iOS and Android.
Segmentation	Control which users & groups will be exposed to a given set of applications and content.
WalkMe MobileInsights™	WalkMe Mobile Insights provides Customers with advanced BI and dashboard capabilities. Customers leverage the analytics tools to better understand user behavior on the supported application(s) in order to determine the areas in need of additional support. Equipped with these insights, content editors can generate the right content to address End User challenges, and then assess the value delivered to the End Users pursuant to their engagement with the WalkMe solutions deployed, and performance on the platform.
WalkMe MobilePrediction AI	WalkMe will monitor and discover user groups likely to perform actions and project a likelihood of conversion.

Visions	
WalkMe Visions™	WalkMe Visions is a tool for measuring and visually investigating user engagement using next-generation digital analytics. Using WalkMe Visions, companies can record, analyze and playback entire End User sessions to find End User-interface pitfalls, streamline bug reporting for QA and R&D uses, and reduce helpdesk and support overhead.

EXHIBIT A-1

TEMPLATE Order (not an actual Order)

Comcast Cable Communications Management, LLC (“Comcast” or “Client”) and [redacted] (“Service Provider” or “Vendor”) have entered into an Access and Services Agreement, dated as of [redacted] (the “Agreement”), relating to the accessing of Services and Technology and Products and performance of Maintenance and Support Services by Service Provider. This Order (“Order”) is made and is effective as of [redacted] (“Effective Date of this Order”) pursuant to the terms and conditions of the Agreement. Capitalized terms not otherwise defined herein have the meaning ascribed to them in the Agreement. In the event of an explicit conflict or inconsistency between the Agreement and this Order, the Agreement will control. **In no event may Intellectual Property Rights and/or pricing be modified in an Order or Statement of Work without the approval of a Comcast employee that is a vice president or more senior.**

- 1. SERVICES/PRODUCTS:
[Insert description]
 - 2. DURATION OF LICENSE (including renewals, if any):
[Insert]
 - 3. START DATE:
[Insert]
 - 4. SERVICES/PRODUCT FEES AND INVOICE SCHEDULE:
[Insert]
 - 5. FEES:
[Insert or Mark Not Applicable]
 - 7. ADDITIONAL TERMS (IF ANY):
[Insert or Mark Not Applicable]
 - 8. CONTACTS:
[Insert for Comcast and Service Provider]
9. Any changes to this Order must be mutually agreed to by the Parties in writing by a Change Order or Addendum to this Order.

AGREED AND ACCEPTED on behalf of the parties by their duly authorized representatives as of the Effective Date of this Order.

COMCAST CABLE COMMUNICATIONS MANAGEMENT, LLC	[NAME OF SERVICE PROVIDER]
By: _____	By: _____
Typed Name: _____	Typed Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

EXHIBIT A-2

Service Provider TEMPLATE Order (not an actual Order)

OFFER VALID THROUGH:

REFERENCE NUMBER:

ACCOUNT EXECUTIVE:

Order Details

Company Name:
Order Form Start Date
Order Form End Date
PO # Required:
If yes, PO #:
If yes, please e-mail the PO to invoices@walkme.com

Billing Cycle:
Billing Cycle Notes:
Payment Terms:
Payment Notes:
Payment Method:

Customer Information

Customer Contact:
Email:
Phone:

Billing Contact:
Billing Email:
Billing Phone:
Invoice sent by:

Billing Address:

WalkMe billing, invoice, and accounts receivables contact: invoices@walkme.com.

Subscription Services	Application		End Users	Monthly Price	Term (in Months)	Total Price
Subscription Services Subtotal						
Additional Services		Quantity	Unit Price			Total Price
Additional Services Subtotal						
			Total Contract Value			

Terms and Conditions:

- When fully executed below, this Order Form shall be governed by the Access and Services Agreement (“Agreement”) with an effective date of September 25, 2020 (the "Agreement"). Capitalized terms not defined on this Order Form have the meanings assigned in the Agreement. In the event of an explicit conflict or inconsistency between the Agreement and this Order, the Agreement will control.
- The Customer hereby acknowledges and agrees that the Services, detailed in Annex 1, must be utilized within the first twelve (12) months of the Order Form Start Date or during the Order Form Term, whichever is less.

Once signed, please return this Order Form to [insert account executive or account manager].

IN WITNESS WHEREOF, the parties have executed this Order Form by their duly authorized officers or representatives.

WalkMe, Inc.

Comcast Cable Communications Management, LLC

Signature: _____
Name: _____
Title: _____
Date: _____

Signature: _____
Name: _____
Title: _____
Date: _____

Exhibit B

WalkMe Service Level Agreement

All references to the “WalkMe Master Subscription Agreement” in this Exhibit B shall be deemed to be references to the Agreement. All references to “Subscription Services” in this Exhibit B shall be deemed to be reference to Services under the Agreement.

1. **Definitions.** Capitalized terms set forth in this Service Level Agreement and not defined below shall have the meanings assigned to them in the WalkMe Master Subscription Agreement.
 - a. **“Coverage Period”** means the period of time during which the System Availability will be measured. Unless otherwise stated, Coverage Period will be equal to a calendar month, expressed in total number of minutes in such month.
 - b. **“Downtime”** means the period of time during which the WalkMe Editor or WalkMe Mobile Console is not available to Customers and/or the WalkMe Player or WalkMe SDK API is not available to End Users.
 - c. **“Excused Downtime”** means any Downtime caused by (i) planned Downtime (of which WalkMe shall give Customer advance notice); (ii) WalkMe’s suspension and termination of Customer’s right to use the Subscription Services pursuant to the terms of the applicable Master Subscription Agreement and/or Order Form; (iii) Customer’s use of the Subscription Services outside the scope permitted or intended by the applicable Master Subscription Agreement and/or Order Form; and (iv) any unavailability caused by circumstances beyond WalkMe’s reasonable control, including, without limitation, any acts of governmental authorities, natural or man-made disasters such as flood, fire, earthquakes, or acts of God, acts of war, acts of terror, civil unrest, strikes or other labor problems (other than those involving WalkMe’s employees, contractors, or agents) hosting facility failures or delays, or denial of service or similar attacks. Note, Customer will be informed of planned maintenance at least one (1) week in advance by an announcement on the log-in screen of the Customer’s account or such otherwise method of notification associated with such Customer’s account.
 - d. **“Potential System Availability”** means the amount of time that a component of the System should be available in a Coverage Period. The Potential System Availability is calculated in minutes and equal to (number of days in the month) x (24 hours) x (60 minutes) – (minutes of Excused Downtime).
 - e. **“System”** means the WalkMe Player, the WalkMe Editor, the WalkMe Mobile SDK API, and the WalkMe Mobile Console, collectively (each may be referred to as a “component” of the System).
 - f. **“System Availability”** means the percentage of time that a respective component of the System is available in a Coverage Period. System Availability is calculated in minutes and equals to (Potential System Availability – Downtime)/(Potential System Availability).
 - g. **“Target Availability”** means the guaranteed availability standards included in the Target Availability Table below.
 - h. **“WalkMe Editor”** means the module in the Subscription Services that allows for the creation of the WalkThrus™ and other WalkMe-generated content.
 - i. **“WalkMe Mobile Console”** means the module in the Subscription Services that allows for the creation of the WalkThrus™ and in-app messages or any other WalkMe-generated content for native mobile applications.
 - j. **“WalkMe Mobile SDK API”** means the module in the Subscription Services that presents all WalkMe-generated and otherwise integrated content visible to the End Customers on native mobile applications.

k. “**WalkMe Player**” means the module in the Subscription Services that presents all WalkMe-generated and otherwise integrated content visible to the End User.

2. **Technical Support.** WalkMe will provide Customer with technical support services (24x7x365), including technical support experts, who will help the Customer troubleshoot any technical questions or issues it encounters with the System (“**Support Services**”). WalkMe will also provide the Customer with online access to its knowledge base and other technical resources at <https://support.walkme.com>.

Customer may contact the WalkMe Support Services by email (support@walkme.com) and/or reach the Support Services at the telephone numbers available at <https://support.walkme.com>:

3. Target Availability Levels

System Target Availability	
WalkMe Player/WalkMe Mobile SDK API Target Availability	99.95%
WalkMe Editor/ WalkMe Mobile Console Target Availability	99.9%

4. Support Response and Resolution Times

Response Time	Target Resolution Time	Priority Level	Description of Defect
Up to 1 hour	4-5 hours	Priority 1	Defect with one or more of the below characteristics occur and there is no workaround: <ul style="list-style-type: none"> • <i>Data corruption</i> – The System will not load or is causing harm to the Customer’s application or website or otherwise materially, adversely affects the Customer’s application. • <i>System hangs</i> - the System hangs indefinitely or there is severe performance degradation, causing unreasonable wait times for resources or response as if the System is hanging. • A main System function supporting a business-critical process has failed, and the System functionality is limited such that critical business processes are paralyzed. • The System crashes repeatedly.
Up to 2 hours	1 day	Priority 2	<ul style="list-style-type: none"> • The System crashes repeatedly and there is a workaround. • The System is usable, but an essential component of the System is malfunctioning and/or substantially impacts business operations. • A critical defect with an acceptable workaround exists.
Within 24 hours	1-2 days	Priority 3	The defect does not seriously affect business operation, causing some minor interruptions. The System is operative with some limitation on minor functions, or minor batch functions are inoperative.
Within 72 hours	2-5 days	Priority 4	Minor mismatch of the specification or aesthetic aspect of the System, which does not impact the usability or effectiveness of the System.
Within 96 hours	5-7 days	Priority 5	Simple questions and requests, which do not affect the System functionality (e.g. documentation issues, feature requests, general questions, etc.).

The Target Resolution Time set forth in the table above shall be subject at all times to Customer's availability and provision to WalkMe of all required information to enable WalkMe to troubleshoot the issue and to access the environment in which the issue has been reported. In addition, the Target Resolution Time set forth above shall only be applicable to issues which do not qualify as product bugs or issues requiring WalkMe to fix its code.

5. Service Credits

- a. If the System Availability of a component of the System is below the Target Availability Levels set forth above ("**Downtime Event**"), Customer may submit a credit request to WalkMe within thirty (30) days of such Downtime Event ("**Service Credit Request**"). In order to initiate a claim for a Service Credit (as defined below), Customer must submit a Service Credit Request in writing and provide sufficient details for WalkMe to validate the Downtime Event, including: (a) Customer's name and contact information; (b) the date and start/end time of the claimed outage(s); and (c) a brief description of the characteristics of the claimed outage(s). The Customer will be notified within ten (10) business days of the written Service Credit Request of the resolution of such Service Credit Request. If the Service Credit Request is rejected by WalkMe, the response notification by WalkMe will specify the basis for such rejection. If the Service Credit Request is approved by WalkMe, WalkMe will issue a Service Credit to Customer's account calculated as a percentage ("**Weighting Factor**") of the total fees payable by Customer to WalkMe during the Coverage Period in which the Downtime Event occurred. The Service Credit shall apply to the next invoice issued by WalkMe or if no additional invoice will be issued then WalkMe shall provide Customer with an extended subscription term proportional to the applicable Service Credit. These Service Credits are Customer's sole remedy for any Downtime Events. If there is a good faith dispute with regard to a Service Credit Request, Comcast will provide Service Provider with written notice detailing the dispute ("Dispute Notice") within sixty (60) days of receipt of the applicable invoice. If Comcast provides a Dispute Notice, then Comcast and Service Provider agree to have a good faith discussion to work to find resolution to the dispute.
- b. The Service Credits will be calculated using the Weighting Factors set forth in the table below:

Service Metric	Service Level	Weighting Factor
WalkMe Player/WalkMe Mobile SDK API Availability	Less than 90% Availability	25%
	90.0 – 96.9% Availability	15%
	97.0% – 98.5% Availability	10%
	98.6% - 99.95% Availability	5%
	> 99.95% Availability	0%
WalkMe Editor/WalkMe Mobile Console	Less than 90% Availability	25%
	90.0 – 96.9% Availability	15%
	97.0% – 98.5% Availability	10%
	98.6% - 99.9% Availability	5%
	> 99.9% Availability	0%

Exhibit C

Fees

Comcast may purchase subscriptions to WalkMe for additional applications in accordance with the Pricing Worksheet below. For further clarification, the tiered pricing below is the cost per end user per month.

If Comcast agrees to enter into a subscription for unlimited application ("ELA"), WalkMe would pro-rate the remaining portion of any of Comcast's current existing subscription and apply that balance towards the purchase of the ELA. An ELA allows Comcast to deploy WalkMe across any number of applications regardless of Tier.

By way of example only, an ELA license for 100,000 end users would permit Comcast to deploy WalkMe across an unlimited number of applications for up to 100,000 end users (or whatever your employee count actually is).

The prices shown below shall remain fixed for any new or existing subscription purchases made within three years from the execution date of this Agreement. Thereafter, WalkMe may raise the prices in the table by no more than 5% per year for two additional years.

Previously licensed applications, WalkMe for Kronos and WalkMe for Workday, as licensed on Statement of Work 2019/06/01 and purchased via Comcast purchase order #2524929, shall renew at the predetermined fees of \$150,000 per year/per application.

Pricing in this table shall apply to Comcast and its affiliates although any affiliates must execute their own Joinder Notice, as set forth in Exhibit G, in order to purchase a subscription.

WalkMe Pricing Worksheet:

Up To # of Users	Tier 3 (internal)- Access only applications which require very low engagement from the user and no input of data	Tier 2(internal) -Data Entry type applications which have considerably lower monthly usage and require data entry level engagement	Tier 1 (internal)- Professional/ departmental or business applications that professional employees engage with almost daily	ELA/Unlimited Applications	External Apps
200	\$ 4.41	\$ 7.50	\$ 10.50	\$ 20.00	\$ 10.4167
500	\$ 1.76	\$ 3.00	\$ 6.00	\$ 20.00	\$ 4.1667
1,000	\$ 1.07	\$ 1.82	\$ 5.50	\$ 20.00	\$ 2.0833
5,000	\$ 0.58	\$ 0.99	\$ 3.00	\$ 12.00	\$ 0.4167
10,000	\$ 0.39	\$ 0.66	\$ 2.00	\$ 11.56	\$ 0.2083
25,000	\$ 0.29	\$ 0.50	\$ 1.68	\$ 9.04	\$ 0.0833
50,000	\$ 0.19	\$ 0.33	\$ 1.20	\$ 6.06	\$ 0.0646
75,000	\$ 0.14	\$ 0.23	\$ 1.07	\$ 5.00	\$ 0.0634
100,000	\$ 0.11	\$ 0.19	\$ 1.00	\$ 5.00	\$ 0.0602
150,000	\$ 0.08	\$ 0.13	\$ 0.80	\$ 5.00	\$ 0.0540
200,000	\$ 0.06	\$ 0.10	\$ 0.70	\$ 5.00	\$ 0.0504
300000 +					\$ 0.0433
500,000					\$ 0.0200
1,000,000					\$ 0.0100
2,500,000					\$ 0.0085
5,000,000					\$ 0.0060

Exhibit D

Data Collection and Targeting Requirements

Service Provider represents and warrants that in connection with its collection and storage of data collected via web beacons, cookies or any other technology that tracks internet usage:

1. Only data that is specifically authorized in writing by Client, or set forth in this Agreement will be collected on Client (which for purposes of this Exhibit D includes affiliates) websites, if Client (or the relevant affiliate) and Service Provider mutually agree to allow Service Provider to set a cookie or otherwise collect data, expiration dates of any cookies will be mutually agreed upon.
2. All data collected is and will continue to be anonymous or immediately anonymized. Unless approved by Client, Service Provider will not collect data that is “personally identifiable” according to any applicable law or regulation;
3. It does not and will not aggregate data collected into databases or engage in any other process that would result in the collation or organization of the data such that the combination or aggregation of data from one or more sources would provide sufficient detail to enable the identification of individual users even if such data was originally collected anonymously;
4. It does not and will not collect any data on health information, credit scores or other types of data designated as “sensitive” data, or data otherwise subject to specific restrictions on collection by law or regulation;
5. It will not aggregate any data it collects or receives and resell or otherwise distribute it in a manner that competes with the advertising services of Client (including, by way of example and not limitation, by claiming to provide data that identifies Client users or user that “look like,” or share characteristics of users of Client services, without necessarily tagging them on Client properties) or as data about, originating from or otherwise related to Client or its customers, and shall not label denote or refer to in any manner the data as having been derived from Client, other than as permitted under this agreement, whether or not such data contains any personally identifiable information;
6. It does and will employ up-to-date, industry recognized “best practices” with respect to technology and procedures to prevent and detect theft, piracy, unauthorized access, copying, duplication or distribution of the data collected from or supplied for use in connection with Client websites.
7. It will notify Client of any breaches of security or incidents of the type described in Section (5) above, within one (1) week of discovery of such incident.
8. Without limiting any of the foregoing, Service Provider does and will comply with all internet privacy and similar laws, rules, regulations, legal orders or decrees and similar promulgations in any applicable jurisdiction (collectively, “Law”) in connection with its collection, use and distribution of data, including without limitation COPPA. In the event of a change of law which is reasonably likely to disrupt Service Providers ability to provide the Services or to continue to collect data of a the same or similar quality, or to prohibit Service Provider’s ability to comply with the provisions of this section, Service Provider will promptly notify Client (including if appropriate, regarding any pending legislation that is reasonably likely to be enacted in the near future) and Service Provider and Client shall negotiate appropriate revisions to or the termination of this Agreement.
9. It will provide a meaningful opportunity for internet users to i) modify the data provided by them; and (ii) opt-out from data collection and targeting by Service Provider and its affiliates and customers, including without limitation, through the Network Advertising Initiatives’ Compliance Program.
10. It will comply, to the extent applicable, with standards for data collection and serving and/or targeting advertising promulgated by self-regulatory and other nationally recognized standards bodies, such as the Interactive Advertising Bureau.

11. There will be no ushering in of other third parties or service providers or otherwise enabling setting of cookies or data collection about Client users including, but not limited to, actions such as cookie synching, unless otherwise agreed to in writing by Client.

12. [Intentionally omitted]

13. It will not grant access to data to any third party except a) on a need to know basis in order to provide specific services to Service Provider; b) after conducting a reasonable investigation of such third party and c) upon entering a written agreement with such third party which contains obligations which are at least as restrictive as the foregoing. In the event the Service Provider collects any data that contains any PII, disclosure of such PII to any third party will be subject to the restrictions set out in Clause 8(d) of the Agreement.

Exhibit E

Information Security Requirements

This Information Security Requirements for Suppliers Exhibit (“Exhibit”) defines certain security controls and requirements for Supplier’s performance of services for, or provision of services or products to, Comcast under the Agreement (“Services”). Unless expressly stated otherwise in the Agreement, the terms of this Exhibit shall take precedence and prevail over any conflicting or inconsistent provisions set forth in the Agreement, statements of work and orders thereunder (collectively or individually, the “Agreement”); *provided, however*, that any security controls specified in the Agreement shall take precedence and prevail over the provisions of this Exhibit where (i) the Agreement expressly states so or (ii) the security controls specified in the Agreement exceed those set forth in this Exhibit. As used herein, “Requirements” means the security requirements set forth in this Exhibit and/or the Agreement (either expressly or to the extent exceeding those set forth in this Exhibit), as applicable.

PART I: Definitions

PART II: Storage, Transmission, Processing and/or Access to Sensitive Non-Public Information

PART III: Supplier Access to Comcast Systems

PART IV: Business Continuity and Disaster Recovery

PART V: Software Development, Web Application Development and/or Web Application Hosting Services that Store or Process Sensitive Non-Public Information and/or are Comcast Branded

PART VI: Additional Requirements Applicable to Parts II and III

I. Definitions. The following definitions apply to these Requirements:

1. Authentication means the process by which a person, process or system is verified as a particular person, process or system or a member of a class of persons, processes or systems, typically for access to data or another right or privilege. Multi-Factor Authentication means Authentication using at least two different verification factors (the factors being something a user knows, something a user has, and something a user is).
2. Cloud Environment means an environment or offering that provides ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
3. Comcast Systems means applications, websites, computing assets, systems, databases, devices, products, or services owned or operated by or for Comcast. Current means an age of one (1) year or less.
4. Days means calendar days unless otherwise specified.
5. Industry Standard means prescribed for use by the National Institute of Standards and Technology (NIST) or aligned with the ISO/IEC 27000 series of standards.
6. Loss means the loss of control over Sensitive Non-Public Information or Personal Information, such that one or more actors may further disclose or Misuse Sensitive Non-Public Information or Personal Information.
7. Misuse means the inappropriate or wrongful exercise of a right or privilege, such as a right or privilege to access information, the wrongful disclosure of that information or the malicious or otherwise improper execution of a function or operation.
8. PCI Data means any and all “cardholder data” (as defined by the prevailing Payment Card Industry Data Security Standard) that Supplier receives, accesses, processes, stores, or transmits on behalf of Comcast.

9. Personal Information means any information that relates to or describes an individual or household, including any data that is linked or linkable to an individual or household.
10. Sanitization means a process that removes information from media or that renders such information irretrievable, consistent with Guidelines for Media Sanitization, NIST Special Publication 800-88 (NIST 800-88), as revised.
11. Secure Destruction means a process that destroys media on which information is located ("Destroyed") and thereby makes recovery of such information impossible, consistent with NIST 800-88, as revised.
12. Secure Transportation means transport utilizing a licensed, bonded, secure carrier that implements and adheres to an Industry Standard chain of custody program, for tracking the movement and disposition of storage media or other equipment from receipt to final disposition.
13. Security Compromise means the unauthorized access, acquisition or use of data, or execution of operations or function through an actual contravention of these Requirements.
14. Sensitive Non-Public Information means any or all of the following:
 - a. Customer proprietary network information ("CPNI");
 - b. Proprietary application source code;
 - c. Non-Supplier access and credential data for any Comcast System;
 - d. Sensitive Personal Information; or
 - e. PCI Data.
15. Sensitive Personal Information means Personal Information that, if subject to unauthorized access or acquisition that compromises the security, confidentiality, or integrity of the personal information, would require notification to a consumer, governmental entity, credit reporting agency, or trigger any other state, federal, or international breach notification laws, and includes, without limitation:
 - a. First name or initial and last name in combination with any of the following:
 1. Social Security Number;
 2. Driver's License Numbers, state identification numbers, passport number, or other government issued ID;
 3. Financial or bank account information (including details of debit/credit cards or other payment instruments);
 4. Health or medical insurance information;
 5. Health or medical conditions (physical, physiological or mental health);
 6. Medical records and history;
 7. Sexual orientation;
 8. Protected Health Information, as defined in Section 164.103 of the Health Insurance Privacy and Portability Act's implementing regulations;
 9. Information collected by automated license plate recognition systems;
 10. Set-top box or other device data, network event data, usage data or activity data generated by a Comcast customer's interaction with any content distributed by or on a Comcast System, or made available by Comcast, information about Comcast customer's visit to (or failure to visit) any website or application;
 11. Biometric information; or
 - b. Username or email address, in combination with a password or security question and answer that would permit access to an online account.
16. Storage Encryption means data encryption in storage using an Industry Standard algorithm.

17. Supplier Devices means devices (computing, storage, telecommunications or networking equipment) operated by or on behalf of Supplier that process, store, or transmit Sensitive Non-Public Information or are used to perform Services.
18. Supplier Systems means any Supplier or its authorized subcontractors' applications, websites, computing assets, systems, databases, devices, products, or services that process, store, or transmit Sensitive Non-Public Information or perform Services.
19. Supplier Staff means employees, contract employees, and temporary staff of Supplier and any authorized subcontractors with access to Sensitive Non-Public Information.
20. Transport Encryption means transport encryption that is no less secure than encryption utilizing the then current IETF (www.ietf.org) ratified version of Transport Layer Security (TLS) protected by a minimum of 128 bit encryption with 1024 bit keys, and in the event Supplier is hosting a web application that is using a Comcast domain, the site must use Comcast-approved digital certificates.

II. **Storage, Transmission, Processing and/or Access to Sensitive Non-Public Information.** In the event Supplier stores, transmits, processes, and/or accesses Sensitive Non-Public Information, Supplier must comply with this Part II and Part VI below.

- A. Access Control. Supplier must utilize logical access controls for all access to Sensitive Non-Public Information, as follows:
 1. Supplier must apply the "Principle of Least Privilege" (or "PLP") model, enabling access only to such Sensitive Non-Public Information and other rights and privileges relating to Comcast operations as are necessary for person or process to perform a legitimate business function.
 2. Supplier shall implement Multi-Factor Authentication for all remote access to Sensitive Non-Public Information hosted by Supplier.
 3. Emergency access processes must be established, with access to emergency accounts controlled.
 4. Except as otherwise approved in writing by Comcast, Sensitive Non-Public Information must be logically isolated from third parties' information.
 5. Supplier must include the use of login/warning banners to provide awareness/notification of restrictions and information security related obligations to Supplier Staff.
 6. Supplier must utilize the following logging and monitoring controls for all Supplier Systems:
 - a. Supplier must maintain electronic logs of all access to Sensitive Non-Public Information, depicting the details of the access.
 - b. Supplier must maintain a security logging and monitoring process which provides for oversight to Supplier compliance or security personnel, and which maintains the integrity of the logs and identifies potential security violations in near-real time.
 - c. All applications and systems security event logs shall be configured to log the creation, deletion, modification or access to Sensitive Non-public Information for forensic analysis and shall be created, retained, and available to Supplier for a minimum of six (6) months either on-line or on backup media. Access events to Sensitive Non-Public Information shall include login success, login failure, logout, session timeout, account lockout, password change, password reset, time and date information, user ID, source IP address and source hostname.
 - d. Logs must be protected from unauthorized access, modification and accidental or deliberate destruction.
 - e. Logs shall be regularly (with the period commensurate with risk) reviewed by Supplier, either manually or using log parsing tools.

- f. Log reviews must be undertaken by a designated trained individual or group of individuals, manually or through the use of tools, in order to detect unauthorized activity. Utilizing NIST Special Publication 800-92 as a guide for log review is encouraged and acceptable.
- B. Asset Management
1. When physically transporting digital media containing Sensitive Non-Public Information, that information must be protected using Storage Encryption, and transported using a qualified courier, with tracking, and in a physically secure container.
 2. When (a) directed by Comcast, or (b) unless specifically otherwise required by law, upon conclusion or termination of the Agreement or when no longer required for Services, Supplier must Sanitize or Destroy (or at Comcast's election return to Comcast) all copies of all Sensitive Non-Public Information, including all backup and archival copies, as well as Sensitive Non-Public Information within Supplier network segments providing Services to Comcast, in any electronic or non-electronic form.
 3. Non-functional electronic storage media (e.g., a failed drive) not capable of Sanitization, must be Destroyed. Supplier shall track disposition of the media (e.g., Destroyed by Supplier, Sanitized by Supplier, conveyed to a Comcast-authorized third party for Destruction, etc.) and store a Certificate of Sanitization (COS) and/or Certificate of Destruction (COD) upon completion of the Sanitization, or Destruction and provide to Comcast upon request.
 4. All hardcopy documents containing Sensitive Non-Public Information must be securely destroyed according to Industry Standards with chain of custody maintained and verification that data destruction was completed.
 5. Supplier shall maintain for no less than one (1) year records which specifically identify the media (or computing assets) that were Destroyed, subject to Sanitization or returned to Comcast, and shall make those records available to Comcast for inspection upon request.
- C. Cloud Controls. Sensitive Non-Public Information must not be processed or stored in a Cloud Environment unless there is Transport Encryption for communications with and among cloud elements.
- D. Compliance
1. For all Cloud Environments, Supplier shall ensure that one organization's data are logically isolated from data of other organizations. Supplier shall further validate, at least once annually, that its third party Cloud Environment providers are compliant with either these Requirements or the Cloud Security Alliance Cloud Controls Matrix (CCM) at <https://cloudsecurityalliance.org>.
 2. In the event Supplier engages in or supports payment card transactions as a part of the Services provided to Comcast, or Services requiring access to or receipt and/or storage of PCI Data of Comcast's customers, Supplier shall comply with the Payment Card Industry Data Security Standard ("PCI DSS"), and any amendments or restatements of the PCI DSS occurring during the term of the Agreement, and shall promptly implement all procedures and practices necessary to remain in compliance with PCI DSS, in each case, at Supplier's sole cost and expense. Supplier will maintain and evidence PCI DSS compliance, and provide Comcast with a copy of Supplier's "Report on Compliance" and "Attestation of Compliance" (as those terms are defined by the PCI Security Standards Council) promptly upon Comcast's request.
 3. Supplier shall maintain a Current SSAE-18 SOC2 Type II, or if a Current SSAE-18 SOC2 Type II is not reasonably available, a SOC3 audit or a Current ISO-27001 certification of Supplier Systems. Upon request from Comcast, Supplier must produce such documentation for Comcast review.
 4. Supplier must ensure retention and restoral of electronic documents (including, without limitation, emails, text messages, and instant messages) when directed by Comcast in connection with actual or anticipated legal proceedings.

E. Communications

1. Supplier must implement the following network security controls for networks that will store, transmit, process and/or access Sensitive Non-Public Information, or otherwise be used in the performance of Services:
 - a. Supplier must employ Industry Standard host or network intrusion detection systems (“IDS”) and intrusion prevention systems (“IPS”) for any environment into which Sensitive Non-Public Information will be placed. Any network IDS or IPS must also be placed on network connection points between the Supplier environment containing Sensitive Non-Public Information and other network environments.
 - b. Suppliers must use automated alerts to detect security events and security alerts must be communicated to authorized personnel to appropriately handle alerts.
 - c. IDS or IPS must be configured with rules appropriate to the environment and otherwise in keeping with Industry Standard configurations. As a default, IDS or IPS alerts must be automated and include at a minimum, alerts for the failure of IDS or IPS, security events and known malware.
 - d. IDS or IPS alerts must be reviewed by trained security personnel with a frequency consistent with the nature of the alert, but at least daily.
 - e. Signatures and software for IDS or IPS must be kept current and up to date.

F. Cryptography

1. All Sensitive Non-Public Information must be stored only using Storage Encryption, when stored on laptops, or workstation hard disks that are not permanently set up with a Supplier facility and magnetic tape media. Sensitive Non-Public Information must not be stored on DVD, CD, removable hard drives, USB drives or similar portable storage.
2. Supplier must use Transport Encryption for Sensitive Non-Public Information that traverses networks outside of the direct control of Supplier (including, but not limited to, the Internet, Wi-Fi and mobile phone networks).
3. Supplier shall document, implement, and maintain enterprise-class encryption key management procedures consistent with Recommendations for Key Management, National Institute of Standards and Technology, NIST Special Publication 800-57 (NIST 800-57), as revised, to ensure the integrity, security, and retrieval of any applicable Comcast encryption keys or Comcast encrypted data.

G. Human Resources

1. Supplier must ensure that Supplier Staff retains no Sensitive Non-Public Information, Comcast information resources or other Comcast property upon request and removal from performing Services.

H. Operations. Supplier must maintain operational controls for all access to Sensitive Non-Public Information, including Supplier Systems hosting Comcast branded web applications, as follows:

1. Supplier must maintain an established change control process, ensuring only authorized changes are applied to systems used to perform under the Agreement or that store, process or transmit Sensitive Non-Public Information.
2. System clocks must be synchronized to a trusted, centralized source clock.
3. Supplier system administrators must review system logs regularly.
4. Security logs must be made available to Supplier security staff.
5. Supplier will conduct network vulnerability scanning on a quarterly basis and after significant changes to Supplier Systems.
6. Supplier will conduct network penetration tests annually and after significant changes to Supplier Systems.

7. Vulnerability management processes must be in place to prioritize vulnerabilities based on the nature/severity of the vulnerability and remediate or mitigate all vulnerabilities as soon as practicable thereafter, but in any event within the following timeframes once the patch, fix or solution has been properly tested (using the manufacture designated rating for third party software and otherwise using Industry Standards such as the Common Vulnerability Scoring System (CVSS) for risk rating):
 - a. Thirty (30) days for critical risk vulnerabilities.
 - b. Sixty (60) days for high risk vulnerabilities.
 - c. Ninety (90) days for medium risk vulnerabilities and seventy five (75) days for PCI assets.
 - d. One Hundred and Eighty (180) to three hundred sixty-five (365) days for low risk vulnerabilities (shorter time frame can be made upon request, on a case-by-case basis for issues identified by Comcast).
8. Upon Comcast's request, Supplier shall provide Comcast with an executive summary of the most recent network vulnerability scan and penetration test as well as evidence of Supplier's vulnerability management processes, which shall validate that security flaws and vulnerabilities are identified and remediated pursuant to the timeframes set forth above.
9. Supplier's use of customized software must be tested for security vulnerabilities using Industry Standards, prior to deployment.
10. Supplier shall use processes consistent with Industry Standards to review and approve the use of commercial off-the-shelf software and open source software and ensure license agreements are in place. Software known to be malicious or carrying malware must not be used.
11. Supplier shall implement data loss prevention (DLP) controls to detect and prevent social security numbers and credit card numbers from being transmitted outside of Supplier Systems without Transport Encryption and Comcast's prior written approval.
12. Supplier must maintain separation/segregation of duties consistent with Industry Standard practices, in order to limit the potential for a single individual to cause excessive harm. Among other things, development functions and environments must be segregated/separated from production operations and environments.
13. Supplier must restrict use of system audit and security tools to authorized staff.
14. Supplier must develop backup plans and schedules to protect against malicious or unplanned destruction of information.
15. In the event Supplier stores, process, or transmits Sensitive Non-Public Information and Comcast does not maintain a copy of such Sensitive Non-Public Information, Supplier will maintain backups of Sensitive Non-Public Information in a secure location for up to three (3) years pursuant to these Requirements, or for such longer timeframe if required by applicable laws or regulations

I. Physical and Environmental Controls

1. Sensitive Non-Public Information contained in paper form or electronic media must be stored in a controlled space (e.g., individual office with a door) with standard, after-business-hours locking; or in locked storage containers (e.g., locked drawer, cabinet).
2. Supplier Systems must be secured from tampering, circumvention or destruction, must be maintained at all times in functional order and must be updated or changed if they become compromised or ineffective (e.g., if keys or access codes are stolen).
3. Supplier's facilities must maintain physical security measures that meet or exceed Industry Standards to prevent and detect physical compromise and include at least the following elements:
 - a. Issuance of temporary or permanent photo identification badges;
 - b. Alarms on all external doors;

- c. Use of CCTV on all entrances/exits; and
- d. Video storage and retention of access records shall be for no less than thirty (30) days for facilities with access to Sensitive Non-Public Information and ninety (90) days for facilities storing Sensitive Non-Public Information
- 4. Supplier must periodically review access records and CCTV video to ensure that access controls are being enforced effectively, with any discrepancies or unauthorized access must be investigated immediately by Supplier.
- 5. For any data center that stores or processes Sensitive Non-Public Information, Supplier must maintain the following environmental controls: climate control, raised floor, smoke, heat and water detection, fire suppression, uninterruptable power supply (UPS), power generators and fire extinguishers.
- 6. If Comcast provides Supplier with its prior written consent to operate call center(s) with access to Sensitive Non-Public Information or Comcast Systems from outside of the United States, then in addition to the controls set forth in this Section II(I), Supplier Staff must work in an area designated for Comcast, and Supplier shall also incorporate the following controls:
 - a. Prohibition of mobile devices;
 - b. Prohibition of applications to save Sensitive Non-Public Information locally;
 - c. Prohibition of paper and writing utensils;
 - d. Disabling of all printing functions;
 - e. Establishment of read-only settings for local drives and folders on workstations to prohibit Sensitive Non-Public Information from being saved locally with the exception of specific drives or folders required for Services-related applications;
 - f. Restriction on use of any external instant messaging, email or social collaboration tools
 - g. Restriction of administrator access on Supplier System end points.
- J. System Development Life Cycle. Supplier shall not use Sensitive Non Public Information in a non-production (test or development) environment.

III. Supplier Access to Comcast Systems. In the event Supplier has access to Comcast Systems, whether or not Supplier has access to Sensitive Non-Public Information, then Supplier shall comply with the Requirements set forth in this Part III and Part VI below:

- A. Access Control
 - 1. Supplier will notify Comcast within twenty-four (24) hours when Supplier Staff no longer require access to Comcast Systems.
 - 2. Upon Comcast's request within six (6) months of the last review, Supplier shall participate in user access reviews for all Supplier Staff who have access to Comcast Systems.
- B. Communications. Where required to render Supplier support under the Agreement, remote maintenance ports and access lists created with the intent of providing remote maintenance must only be enabled during the needed support window, and must be disabled when the support window closes. Supplier shall provide all assistance and cooperation reasonably necessary to facilitate Comcast's monitoring of any such access.
- C. Third Party Connections
 - 1. Supplier must only access Comcast Systems as necessary to perform Services.

2. All Supplier Devices to be used to connect to a Comcast network remotely must be either provided by Comcast or alternatively must be owned or leased and managed by the Supplier or permitted subcontractors. Personally-owned equipment may not be used to perform Services.
3. Supplier Devices must not connect directly to the Comcast enterprise network or enterprise wireless network outside of approved remote connections.
4. Unless otherwise approved or directed by Comcast, all remote access (i.e. access from outside a Comcast owned or controlled facility) to a Comcast network must utilize approved Comcast virtual private networks, Transport Encryption and Multi-Factor Authentication.
5. As between Supplier and Comcast, Comcast shall control all access control mechanisms used to restrict access to Comcast's internal business network and Comcast Systems.
6. All Supplier network traffic that passes through Comcast's firewalls must only utilize the defined protocols and services required to provide the intended functionality.
7. If Supplier exchanges data through Comcast's firewalls, Supplier shall work with Comcast to document the access and establish specific ports, rules and protocols acceptable to Comcast.
8. Supplier must not bypass or attempt to circumvent established Comcast security controls, including when accessing external networks from a Comcast System.
9. Comcast may terminate Supplier's access to any Comcast System without notice, if Comcast believes that such access is adversely affecting the security of Comcast or Comcast Systems.

IV. Business Continuity and Disaster Recovery. In the event the Agreement requires Supplier to maintain a recovery time objective (RTO) of less than 72 hours Supplier shall comply with the Requirements in this Part IV.

1. Supplier must have a disaster recovery (DR) program and maintain a documented organizational business continuity plan (BCP). The program and plans must be designed to ensure that Supplier can continue to function through operational interruption and continue to provide Services.
2. Supplier must ensure that the scope of the BCP covers all locations, personnel and information systems that are used to perform Services.
3. The DR plan and BCP must be minimally tested on an annual basis. Supplier must document the results, and upon request, Supplier will provide documentation for Comcast's review to confirm that tests are being performed.
4. Supplier must promptly notify Comcast in the event the DR plan and/or BCP is executed and report the potential impact on Supplier's capability to perform Services.

V. Supplier Provision of Software Development, Web Application Development and/or Web Application Hosting Services with access to Sensitive Non-Public Information and/or uses a Comcast Registered Domain Name. In the event Supplier provides software or web application development and/or web application hosting Services with access to Sensitive Non-Public Information and/or uses a Comcast domain, Supplier shall comply with the Requirements set forth in Section VI(C)(1)(3) as well the Requirements in this Part V.

- A. Access Control. Supplier must implement Comcast single sign on (SSO) authentication for all web applications that are accessible by Comcast personnel.
- B. Communications

1. Applications hosted on behalf of Comcast that provide services via the Internet must reside in a DMZ (DMZ designs as defined in NIST Special Publication 800-41, Guidelines on Firewalls and Firewall Policy, are acceptable).
 2. System components that store Sensitive Non-Public Information, such as a database, must be placed in a internal network zone, segregated from the DMZ and other untrusted networks.
 3. Access via web applications must utilize Transport Encryption controls.
 4. Administrator and privileged access to web applications must utilize Multi-Factor Authentication.
 5. Unless otherwise directed by Comcast, Supplier shall not present identifying information such as Comcast's name, logo or address before a successful login into a system hosted by Supplier for Comcast.
- C. Compliance. In the event Supplier is hosting web applications on behalf of Comcast, Supplier will decommission all applications upon expiration or termination of the Agreement.
- D. Software Development Life Cycle
1. Supplier must utilize the following application management controls:
 - a. Regardless of development methodology (traditional, agile, other), Supplier must maintain a software development life cycle ("SDLC") process that incorporates security vulnerability and malicious code assessments throughout each stage of the development process.
 - b. Supplier Staff shall receive regular training on coding and design in application security.
 - c. Within the Supplier's SDLC, a security vulnerability and malicious code assessment must be performed prior to initial application deployment.
 - d. Application development activities must not occur on Supplier Systems that also perform live production operations.
 - e. Application source code can only be permanently stored on systems dedicated to the storage of source code (such as a source code repository) that includes logs of all updates to code maintained. Permanent storage of source code on laptops, desktops and other mobile computing devices is prohibited.
 - f. Access to the application source code must be limited to Supplier Staff in accordance with PLP.
 - g. Application source code must be maintained using version control.
 - h. Application documentation must be kept up to date, held in accessible form, and protected from loss or damage.
 - i. Information security requirements must be integrated with the design and specification documentation for Supplier Systems.
 - j. Supplier must subject operating system, software and firmware updates to a security review to screen for vulnerabilities and to verify the source of the items, prior to implementation, and be able to validate that the update is from an approved source.
 - k. Supplier will perform security testing of application open source code, and remediate security flaws prior to production implementation.
 2. Supplier will conduct security testing consistent with Industry Standards for all software developed or customized for Comcast and remediate any security flaws identified.
 3. Supplier will develop web applications in compliance with Open Web Application Security Project (OWASP) Application Security Verification Standard. Web Applications will be reviewed for the presence of the OWASP Top Ten.
 4. At least annually and prior to implementing significant changes to any hosted web application, Supplier will either (i) cooperate with Comcast to conduct static code analysis scanning, dynamic scanning and penetration testing of the application (collectively "Scans") or (ii) provide to Comcast the current report of the Scans completed by Supplier.

5. Supplier will remediate security flaws and vulnerabilities identified in application security tests according to the time frames outlined in Sections II(H)(7)(a)-(d).
- VI. **Additional Requirements Applicable to Parts II and III**. The following Requirements shall apply to Part II (Storage, Transmission, Processing and/or Access to Sensitive Non-Public Information) and Part III Supplier Access to Comcast Systems):
- VII. **[Intentionally omitted]**
- VIII. **Access Control**. Supplier must utilize logical access controls for all access to Sensitive Non-Public Information or Comcast Systems, as follows:
 - IX. A PLP process that requires (i) termination of access by Supplier Staff which no longer requires access to perform Services within one (1) calendar day of termination, and (ii) notification to all affected Supplier information system and personnel managers within one (1) business day of such employee/contractor status changes (e.g. transferred or reassigned).
 - X. A process of controlling user IDs and other identifiers to ensure they are unique among users and are not shared.
 - XI. Industry Standard password selection and aging procedures to limit opportunities for compromise of password security must be utilized and must at least include the following controls:
 - XII. Limit repeated access attempts by locking out the user ID after not more than five (5) attempts.
 - XIII. Verification of user identity before any password resets.
 - XIV. If a session has been idle for more (i) than fifteen (15) minutes for administrator consoles, (ii) thirty (30) minutes for remote access or external Supplier Systems with access to Sensitive Non-Public Information, or (iii) sixty (60) minutes for internal Supplier Systems, require the user to re-enter the password to reactivate the terminal.
 - XV. Control and encrypt passwords using Storage Encryption to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect.
 - XVI. Password changes must be accomplished through a secure procedure.
 - XVII. Passwords must never be transmitted in clear text.
 - XVIII. Display and printing of passwords must be masked.
 - XIX. Passwords are at least 8 characters and have: upper case letters, lower case letters, westernized Arabic numerals (1, 2,9), non-alphanumeric (special) characters (e.g. ?, |, %, \$, #, etc.) and equivalent international language representations.
 - XX. Passwords cannot be identical to the last eight (8) previously used passwords.
 - XXI. Passwords have a maximum validity of ninety (90) days.
 - XXII. Default, temporary or pre-set passwords are set to unique values and changed immediately after first use.
 - XXIII. Minimum password age must be set to three (3) days or greater.
 - XXIV. Shared or elevated privileged accounts shall not be used unless the usage can be reliably tracked back to an individual Supplier Staff person.
 - XXV. Accounts remaining inactive for ninety (90) days must be disabled.
 - XXVI. Supplier shall verify continued entitlement to access consistent with PLP at least annually (and at least every ninety (90) days for elevated privilege or administrator accounts for applications/systems/databases), using processes that provide independent assurance.
 - XXVII. To prevent disclosure of Sensitive Non-Public Information when unnecessary to perform a required business function, Supplier shall mask or truncate payment card number and passwords in display.
 - XXVIII. Supplier must implement mobile device management (MDM) controls for all mobile devices with access to Sensitive Non-Public Information and/or Comcast Systems that include passwords with at

least six (6) characters, automated lockouts after fifteen (15) minutes, device encryption and remote wipe capabilities in the event the device is lost or stolen.

A. Asset Management. Supplier will maintain an inventory of assets (computers, firewalls, routers, security devices, filing cabinets, etc.) that collect, store, process, access or transmit Sensitive Non-Public Information and/or have access to Comcast Systems.

B. Compliance.

1. Supplier shall reasonably cooperate with Comcast's efforts to verify Supplier's compliance with these Requirements, which efforts may include periodic audits (not to exceed one (1) audit in any twelve (12) month period) of Supplier's operations, including onsite validation at a Supplier facility dedicated to providing Services to Comcast, by Comcast or a third party at Comcast request and on reasonable notice, and Supplier will remediate any critical security issues discovered by Comcast that are associated with the Services within thirty (30) days, and provide a commitment to Comcast within thirty (30) days to address any other security issues in a timely manner.
2. Supplier shall reasonably cooperate with Comcast's inquiries regarding security vulnerabilities identified through Comcast's use of third party monitoring tools.
3. Supplier shall provide periodic updates and evidence of remediation of security issues upon Comcast request.
4. Supplier shall provide periodic updates at Comcast's request related to the identification and remediation of publicly disclosed information security threats and vulnerabilities on Supplier Systems.
5. Supplier shall also participate in all regulatory or governmental inquiries or investigations relating to the Agreement, as reasonably requested by Comcast.
6. Supplier Staff must complete information security awareness training on an annual basis with a focus on common security themes and provide a summary of the training to Comcast upon request.
7. Supplier Staff must attest to a Supplier Systems acceptable use policy (AUP) on an annual basis and provide a copy or summary to Comcast upon request. The AUP should include a right to monitor, proper handling of sensitive information, personal use of corporate assets, social engineering vigilance, and activities that are prohibited.

2. [Intentionally omitted]

C. Communications.

1. Supplier must implement the following network security controls for networks:
2. Servers that are accessible from untrusted networks must be isolated from servers on trusted networks.
 - a. Third party connections to Supplier's networks must be monitored and reviewed by Supplier to ensure authorized access and appropriate usage.
 - b. All routers and firewalls must be configured using Industry Standard secure configurations with firewall rulesets reviewed annually.
 - c. Supplier must implement firewall controls at each Internet connection and between any Demilitarized Zone (DMZ), if applicable, and/or the Supplier's internal network to control the ingress and egress of communications.
 - d. Remote access to Sensitive Non-Public Information from a location outside of Supplier's facilities must use an Industry Standard virtual private network (VPN) connection including Transport Encryption.

- e. Supplier supplied default passwords must be changed and unnecessary default accounts must be disabled prior to implementation.
- f. Supplier must maintain data flows and network diagrams as they relate to any Services subject to Part II.

D. Incident Management

1. Supplier must include in its information security a plan for security incident management and response in the event of (i) Security Compromise with respect to Personal Information, Sensitive Non-Public Information or any operations providing services to Comcast, (ii) other loss or misuse of such information or (iii) malware computer virus, system malfunction, network attacks and intrusions posing a significant threat to such information or any operations providing services to Comcast (each, a "Security Incident"). The Supplier shall forthwith initiate such security incident plan and take remedial actions therein when there is a Security Incident.
2. Supplier must provide notification via electronic mail to SecurityFusionCenter@comcast.com of a Security Incident described in Sections E(1)(i) and (ii) above as soon as practicable after, but no later than twenty-four (24) hours, following awareness of the Security Incident.
3. For any Security Incident, Supplier must provide regular updates to SecurityFusionCenter@comcast.com or, if directed by Comcast, to a security point of contact specifically designated by Comcast for the Security Incident, and shall cooperate with Comcast or its regulators in its efforts to investigate the same.
4. For any Security Incident involving the Services, Comcast employees, customers, or prospective customers, Comcast shall exclusively control the provision of any notices concerning such Security Incident to any person affected or potentially affected thereby and applicable domestic and international authorities.
5. Supplier must be available to respond to Security Incidents twenty-four (24) hours a day, seven (7) days a week.
6. Supplier must fully cooperate with Customer in reporting a Security Incident or a threatened Security Incident to the competent government authorities and notify the relevant data subjects and other stakeholders to the extent required by any applicable laws.

E. Operations. Supplier must maintain operational controls:

1. Supplier shall maintain policies and standards for the secure build of desktops, laptops, servers, networks, and mobile devices.
2. Standard operating procedures must exist for a security patch management process to ensure patches are applied in a timely manner and a repeatable, prioritized and standardized way for all software layers for all Supplier Devices and Supplier Systems.
3. Supplier must implement Industry Standard anti-virus/malware software operating in real time on all servers, laptops and desktops.
4. Anti-virus libraries must be updated at least once per day.
5. A full scan of all files on local drives must be conducted at least once every four weeks on laptops and desktops
6. A full scan of all systems and boot files, drives, registry and memory must be conducted at least weekly on servers.
7. Supplier must disable or restrict unnecessary functions, services, utilities and commands on systems.

F. Physical and Environmental Controls. Supplier's facilities must maintain physical security measures that meet or exceed Industry Standards to prevent and detect physical compromise and include:

1. Use of smartcards or other electronic or physical identity verification systems (pin/key access locks, biometrics, etc.);
2. Escorting of visitors;
3. Windows must be constructed in a manner that prevents them from being opened or at a minimum use locks;
4. Use of structures/containment resistant to physical compromise; and
5. Supplier's procedures must assure that access to a facility is removed promptly when no longer required or appropriate (e.g., reassignment of personnel, termination of employment).

G. Policy Management

1. Supplier must (i) have or establish documented information security policies and standards approved by Supplier's executive management ("Supplier's Security Standards") that meet these Requirements and conform to all applicable data protection laws and regulations, and (ii) designate one or more qualified Supplier employees with responsibility to maintain the Supplier information security program.
2. Supplier must regularly review, at least annually, Supplier's Security Standards, including whenever there is a material change in business practices.

H. Supplier Relationships

1. Supplier must require all permitted subcontractors to comply in writing with obligations substantially similar to these Requirements, and shall provide written evidence of such written compliance to Comcast promptly upon request.
2. Supplier shall conduct periodic reviews of permitted subcontractors' security controls to determine that such controls are in compliance with these Requirements. In the event Supplier identifies deficiencies in any subcontractor's security controls, Supplier shall maintain a report of such findings and ensure that such deficiencies are remediated within reasonable timeframes, commensurate with their severity.

Exhibit F

Termination Assistance

Termination Assistance Services. Unless otherwise agreed to by the Parties in writing, commencing on the effective date of any notice of termination or non-renewal of this Agreement (or such other date as mutually agreed by the Parties), and continuing until three (3) months thereafter (the "**Wind Down/Transition Period**"), Service Provider will provide to Client, such reasonable cooperation, assistance and services as more fully identified below (the "**Wind Down/Transition Services**"). Upon any termination of this Agreement for breach by Service Provider pursuant to Section 13, the Wind Down/Transition Services shall be provided at no additional charge to Client.

Service Provider will provide all information and assistance reasonably required to assure the smooth transition and/or migration of Client and Client Data to the corresponding systems of Client or a third party provider designated by Client, in accordance with a process and schedule reasonably defined by Client ("**Wind Down**"). Wind Down services will be provided by Service Provider as a professional service with fees payable by Client in accordance with the professional services rates of \$200 per hour. The Wind Down will begin at a Client specified date and Client may terminate the Wind Down at any time for any reason upon notice. The Parties acknowledge and agree that such assistance shall include Service Provider providing a complete copy of all Client Data (current as of the last day of the Wind Down Period) in an electronic format reasonably specified by Client such that it may be migrated by Client to such other systems.

Exhibit G

Joinder Notice

As of this [redacted] day of [redacted], 201[redacted] (“Effective Date”), [Comcast entity joining] (“Comcast Affiliate”) desires to execute this Notice of Joinder (“Joinder Notice”), whereby Comcast Affiliate shall be deemed a “Client” under that certain Access and Services Agreement entered into between [redacted], a [redacted] corporation and Comcast Cable Communications Management, LLC, a Delaware limited liability company and dated as of [redacted] 201[redacted] (“Agreement”).

NOW THEREFORE, pursuant to the provisions of Section 17(c) of the Agreement:

1. Comcast Affiliate hereby represents and warrants that Comcast Affiliate is an “Affiliate” of Comcast Cable Communications Management, LLC as defined under the Agreement.
2. As of the Effective Date, Comcast Affiliate shall be deemed a Client under the Agreement.
3. Comcast Affiliate and [redacted] shall be individually liable to each other for any obligations or breaches of representations, warranties or obligations of the other pursuant to the Agreement.

[insert name of Comcast Affiliate]

By: [redacted]
Name: [redacted]
Title: [redacted]

Agreed and Accepted this ____
Day of _____

[INSERT PROPER CORPORATE NAME OF SERVICE PROVIDER]

By: [redacted]
Name: [redacted]
Title: [redacted]

EXHIBIT H-1

Limitation on Use of Personal Information; Consumer Requests

- I. **Limitations on Use of Personal Information.** Client may disclose Personal Information (defined below) to Service Provider for the purpose of Service Provider performing services on behalf of Client or providing products as described in the Agreement(s). Service Provider agrees that with regard to all Personal Information collected, processed, stored or transmitted by, or accessible to, Service Provider in the course of the Agreement(s), Service Provider will process such Personal Information only on behalf of Client, according to the directions set forth by Client. Service Provider further agrees that Service Provider will not retain, use, or disclose any Personal Information provided by or on behalf of Client or collected by Service Provider on Client's behalf for any purpose other than (i) providing the services and/or products under the Agreement(s) and (ii) using the Personal Information internally to verify or maintain the quality or safety of the services and/or products, and to improve, upgrade or enhance the services either for Client or for Service Provider's customers generally. Service Provider acknowledges that it is prohibited from: (a) selling the Personal Information; (b) retaining, using, or disclosing the Personal Information for any purpose other than providing to Client the services and/or products specified in the Agreement(s); or (c) retaining, using, or disclosing the Personal Information outside of the direct business relationship with Client. Further, Service Provider certifies that it understands and will comply with the restrictions contained herein. Service Provider shall ensure that Service Provider's subcontractors who collect, process, store, or transmit Personal Information on Service Provider's behalf agree in writing to the same restrictions and requirements that apply to Service Provider through this Exhibit A and the Agreement(s) with respect to Personal Information, including complying with the applicable requirements of the Privacy Laws. Upon request, Service Provider will fully cooperate in the prompt completion of reasonable privacy and/or security assessments performed by Client or its contractor related to Service Provider's or Service Provider's subcontractors' access, use, and/or storage of Personal Information, including but not limited to providing information about Service Provider's policies, practices, and controls.

- II. **Consumer Requests.** Service Provider will implement and maintain sufficient processes and procedures to satisfy Client's requests related to consumers' rights to opt-out, modify, access, and/or erase their Personal Information as required by all applicable Privacy Laws. Within ten (10) days of a written request from Client (email sufficient), Service Provider will, as applicable, (i) implement any requested modifications, opt-outs and cease any use of the Personal Information; (ii) provide information requested by Client about Service Provider's use of the Personal Information (including, but not limited to, the categories of Personal Information that were collected and categories of subcontractors to whom Service Provider has disclosed the Personal Information); (iii) provide the specific pieces of Personal Information that Service Provider has collected or otherwise obtained about the consumer on behalf of Client; (iv) if the Personal Information is maintained in an electronic format, provide it in a portable and, if technically feasible, in readily usable format that allows the consumer to transmit the information to another entity without hindrance; and (v) securely erase or destroy the Personal Information, including any copies maintained by any Service Provider subcontractor.

- III. **Security.** Without limiting or abridging any security or other requirements set forth in the Agreement(s), if Service Provider receives any Sensitive Personal Information (defined below), then Service Provider agrees to implement, and cause any of its subcontractors providing services under the Agreement(s) to implement, a comprehensive security program that (i) includes administrative, physical and technical safeguards to protect all Sensitive Personal Information, (ii) meets or exceeds accepted industry practices for the protection of highly sensitive information, and (iii) at a minimum, conforms to the information security requirements set forth in **Exhibit E**.

Definitions.

"Personal Information" is defined in **Exhibit E**.

“Privacy Laws” means all laws, rules, regulations, decrees, or other enactments, orders, mandates, or resolutions relating to privacy, data security, and/or data protection, and any implementing, derivative or related legislation, rule, and regulation as amended, extended, repealed and replaced, or re-enacted, as well as any applicable industry self-regulatory programs (including the Digital Advertising Alliance Self-Regulatory Principles) related to the collection, use, disclosure, and security of Personal Information.

“Sensitive Personal Information” is defined in **Exhibit E**.

EXHIBIT H-2

Data Processing Addendum

This Data Processing Addendum (this “*Addendum*”), is part of the **Access and Services Agreement, dated September 25, 2020 (“Agreement”)** between **WalkMe, Inc. (“Company”)** and **Comcast Cable Communications Management, LLC (“Comcast”)** and governs Company’s Processing of Personal Information in connection with the Agreement.

1. Except as expressly stated otherwise, in the event of a conflict between the terms of the Agreement and the terms of this Addendum, the terms of this Addendum will take precedence to the extent necessary to resolve the conflict.
2. This Addendum applies to each agreement between Comcast and Company under which Company Processes Personal Information as part of performing under that agreement.
3. The Addendum will be effective on the last signature date set forth below.
4. The attachments referred to herein will be construed with, and as an integral part of, this Addendum.

6. Definitions

- 6.1. Terms that are capitalized but not defined have the meanings assigned to them in the Agreement.
- 6.2. The following terms have the meanings assigned to them in the GDPR: “*Controller*” and “*Processor*.”
- 6.3. “*General Data Protection Regulation*” (“*GDPR*”) means Regulation (EU) 2016/679.
- 6.4. “*Law*” means any applicable law, rule, regulation, decree, statute, or other enactment, order, mandate or resolution relating to data security, data protection and/or privacy, including the GDPR, and any implementing, derivative or related legislation, rule, and regulation as amended, extended, repealed and replaced, or re-enacted.
- 6.5. “*Personal Information*” means information provided to Company by Comcast or that Company creates, collects, or otherwise Processes on behalf of Comcast, that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer, Comcast employee, or household, and includes information that is lawfully made available from federal, state, or local government records.
- 6.6. “*Process*” and its cognates means any operation or set of operations that is performed on Personal Information, including storage, disclosure, erasure, and destruction.
- 6.7. “*Standard Contractual Clauses*” (“*SCCs*”) means the European Union standard contractual clauses for the transfer of personal data from the European Economic Area to third countries. Unless otherwise specified, a reference to “*SCCs*” means the controller-to-processor version (Commission Decision 2010/87/EU) or the controller-to-controller version (Commission Decision 2004/915/EC), as context requires.
- 6.8. “*Subprocessor*” means any entity that Processes Personal Information on behalf of Company to assist Company in its performance of the Agreement.

7. Status of the Parties and Scope

- 7.1. The parties agree that, with respect to all Personal Information and purposes of Processing described in Appendix 1a, Comcast is a Controller, and Company is a Processor.

8. Obligations of Company

- 8.1. **Instructions.** Company will only Process Personal Information on documented instructions, which include the Agreement and this Addendum, from Comcast and not for any other purpose unless required to do so by applicable law. Company will promptly inform Comcast if following Comcast’s instructions would result in a violation of applicable law or where Company must disclose Personal

Information in response to a legal obligation, unless the legal obligation prohibits Company from making such disclosure.

Without prejudice to Comcast's other rights and remedies under applicable laws or the Agreement, if Company fails to Process Personal Information pursuant to the Agreement or this Addendum or fails to perform any Personal Information protection obligations under the law, Company shall, with or without Comcast's notice, cease its breaches and take remedial measures immediately to mitigate or remove the security risks.

Company's breach of this Addendum or relevant Personal Information protection and cyber security provisions in the Agreement will be regarded as a material breach of the Agreement which will entitle Comcast to terminate the Agreement pursuant to Section 13 (Term; Termination) of the Agreement.

- 8.2. **Individuals' Requests.** Company will implement and maintain technical and organizational means to obtain information necessary to enable Comcast to respond to requests from individuals to exercise rights afforded to them under Law or applicable Comcast privacy policies, including rights of access, deletion, modification, portability, opt-out, limitation of processing, or objection. Company will notify Comcast without undue delay of an individual's request to exercise his or her rights. At Comcast's instruction, Company will produce the information necessary to facilitate Comcast's response to the requesting individual, and Company will provide such information within ten (10) days of the instruction. If Company is unable to carry out Comcast's instruction, or is unable to carry out the instruction within the specified period, it will immediately notify Comcast and provide the reason.
- 8.3. **Governmental Requests.** If Company receives any type of request or inquiry from a governmental authority (*e.g.*, the Federal Trade Commission, the Attorney General of a U.S. state, Cyberspace Administration of China (CAC), or a European data protection authority) in connection with the parties' Processing of Personal Information, Company will immediately inform Comcast and will reasonably cooperate to provide Comcast with records related to its Processing activities in connection with the Agreement, including information on the categories of Personal Information Processed and the purposes of the Processing, the use of Subprocessors with respect to such Processing, any data disclosures or transfers to third parties, and a general description of technical and organizational measures used to protect the security of such data.
- 8.4. **Cooperation.** Company will reasonably cooperate with Comcast: (i) to ensure compliance with security requirements in Law applicable to Personal Information; (ii) to ensure compliance with Law applicable to Security Breach notification obligations; and (iii) in connection with Comcast's requests related to data protection impact assessments and consultation with supervisory or other governmental authorities.
- 8.5. **Subprocessing.** Company may not engage any Subprocessor without the prior written consent of Comcast. Where Company engages a Subprocessor for carrying out specific Processing activities on behalf of Comcast, Company will impose on that Subprocessor the data protection obligations that are consistent with this Addendum and Law. Where that Subprocessor fails to fulfil its data protection obligations, Company will remain fully liable to Comcast for the performance of that Subprocessor's obligations.

Subject to the preceding paragraph, if Company engages a Subprocessor to Process Personal Information, Company shall conduct a Personal Information security assessment(s) against such Subprocessor to ensure that the Subprocessor will meet the Personal Information protection and security requirements under the Agreement, this Addendum and applicable laws. Company shall accurately record and store information in relation to engaging Subprocessors including all Personal Information security assessment documents and shall provide the same to Comcast upon request.
- 8.6. **Deletion or Return.** Notwithstanding Section 8(k) of the Agreement, upon the expiration or termination of the Agreement or Comcast's request, Company will return all Personal Information to Comcast or at Comcast's option, destroy all Personal Information and provide within ten (10) days of Comcast's request a written certification signed by an officer of Company, certifying that all Personal

Information in all formats, including without limitation, paper, electronic and disk form, have been returned or destroyed, as the case may be.

- 8.7. **Transfer of Personal Information.** Except as set permitted under the Agreement, Company may not transfer, store, or Process Personal Information (i) outside of the United States ; or (ii) to any third party, without Comcast's express prior written permission.

8.8. **Cross-border Data Transfer**

Data Transfers from the European Economic Area, United Kingdom, or Switzerland to the United States. To the extent that one party receives Personal Information at its facilities in a country that has not been designated by the European Commission or Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for Personal Information from the other party in the EEA, United Kingdom, or Switzerland, the parties will comply with the obligations of the form of SCCs applicable to the parties' status as either data importer or data exporter. Appendix 1 sets forth the parties' statuses and respective obligations and the information required by the SCCs' Annexes. The SCCs are hereby incorporated into this Addendum, and the parties agree that by executing this Addendum they are accepting their respective obligations under the SCCs; provided that if the receiving party is in the United States and has an active certification under the EU-U.S. Privacy Shield program, it may use that certification in lieu of the SCCs. If the receiving party loses its EU-U.S. Privacy Shield program certification, or the certification becomes invalid for any reason, the parties agree that they will have been deemed to have executed the SCCs. Notwithstanding anything to the contrary in the Agreement or the Addendum, in the event of a conflict the SCCs will take precedence. To the extent Company receives Personal Information at its facilities outside Australia from a Comcast Affiliate that carries on business in Australia, Company undertakes that it will not engage in conduct in respect of that Personal Information which would breach an Australian Privacy Principle (as defined in the Australian Privacy Act 1988) if that conduct had occurred in Australia.

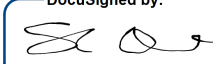
Data Transfers from the People's Republic of China to a foreign country or region. To the extent that one party receives Personal Information at its facilities in a country or region outside of the People's Republic of China from the other party or its affiliates in the People's Republic of China, the parties shall also comply with the obligations as either data importer or data exporter set forth in Appendix 2.

- 8.9. **Confidentiality.** Company will restrict access to Personal Information to those authorized persons who need such information to provide services under the Agreement. Company will ensure such authorized persons are obligated to maintain the confidentiality of any Personal Information.
- 8.10. **Security.** Company will implement technical and organizational measures and good industry practices to ensure the security of Personal Information. Such security measures will be at least as protective as the security requirements set forth in the Agreement.
- 8.11. **Breach Notification.** In addition to the requirements of Section 8(f) of the Agreement , after becoming aware of a Security Breach affecting Personal Information under this Agreement, Company will notify Comcast immediately and make best efforts secure its systems immediately. Company will not make any notification to regulatory authorities or individuals unless Comcast has given Company express written permission or such notification is required by applicable law.
- 8.12. **Audits.** Upon request, and in addition to the requirements of Section 8(f) the Agreement, Company will make available to Comcast all information necessary, and allow for and contribute to audits, including inspections, conducted by Comcast or another auditor mandated by Comcast, to demonstrate compliance with Law. Comcast will treat all such information as Confidential Information consistent with the terms of the Agreement.

The parties' authorized signatories have duly executed this Agreement:

COMPANY

**Comcast Cable Communications
Management, LLC**

DocuSigned by:

Signature: 10B8933FF9F6495...
Title: CRO
Print Name : Shane Orlick
Date: 9/29/2020

Signature: _____
Title: _____
Print Name : _____
Date: _____

Appendix 1 to Data Processing Addendum: Information Required by SCCs

1. The Parties' Roles

- 1.1. The parties agree that, with respect to the Controller-to-Processor SCCs (Commission Decision 2010/87/EU), Comcast is a data exporter and Company is a data importer regardless of their location.

2. Applicable SCCs Provisions

- 2.1. The parties agree that, with respect to the Controller-to-Processor SCCs (Commission Decision 2010/87/EU), for the purposes of Clauses 9 and 11(3), the governing law will be the country in which the data exporter is established.

Appendix 1a to Data Processing Addendum

The following chart includes the information required by Appendices 1 and 2 of the controller-to-processor standard contractual clauses and Annex B of the controller-to-controller standard contractual clauses.

Categories of Personal Information	<p>Any Personal Information that Company Processes on behalf of Comcast pursuant to the Services (as defined in the Agreement).</p> <ol style="list-style-type: none"> 1. Categories of information and data we may collect from our End Users. <ul style="list-style-type: none"> ○ <u>Passive Collection</u>. Passively Collected Information means any information which is available to WalkMe while End Users are using the Service. Passively Collected Information consists of technical information and behavioral information (i.e. the interaction of the End User with the Service), including, but not limited to, the End User's operating system, type of browser, screen resolution, font type, time zone, Flash version, the End User's 'click-stream' on the Service, the period of time the End User utilized the Services, etc. ○ <u>Personal Information</u>. Personal Information means any information that relates to or describes an individual or household, including any data that is linked or linkable to an individual or household. By default, the WalkMe System™ does not collect any Personal Information, other than IP addresses in logs for security purposes, End Users' geolocation (country and city in which you are located) and masked IP addresses for the ongoing operation of the WalkMe System, any of which may be considered as Personal Information in some jurisdictions. For more information, please see below. 2. The WalkMe System™ utilizes certain identifiers retained in a cookie file as detailed below. Such identifiers are not linked to any Personal Information about an End User and may also be stored (without any link to Personal Information) on WalkMe's servers. 3. WalkMe may also collect the email addresses of people who communicate with WalkMe via email or create accounts and login credentials. 4. Special Features. Customer may use certain features which may cause the system to collect and store additional Personal Information ("Special Features"). These Special Features may include: <ul style="list-style-type: none"> ○ <u>User Behavior Tracking</u>: a feature which allows Customers to track End User's interaction with HTML elements on an application or webpage for which the End User clicked on, including the following information: (i) End User IP address; (ii) URL; (ii) page title; (iii) text, value and description of each element the End User clicked on (excluding any inputted information that is in a credit card number format); and (iv) snapshot of Canvas elements (drawable regions defined in HTML code) which may be available on an application or webpage. ○ <u>Screenshot Settings</u>: a feature which allows Customers to capture screenshots of the application or webpage including the WalkMe content. For instance, a Customer
---	---

	<p>may capture a WalkThru™ as it appears on the user interface of the Customer's application.</p> <ul style="list-style-type: none"> ○ Custom Variables: a feature which allows Customers to track End Users by an available HTML element, variable or cookie and which may be used to distinguish between segments of End Users. For instance, a Customer may use a custom variable to provide certain WalkMe content to only a particular set of End Users. ○ Custom User Identifier: a feature which allows Customers to track End User Identifier by an available HTML element, variable or cookie. ○ Adaptive Element Recognition: a feature that improves element recognition accuracy over time, which on rare occasions may capture a page snapshot and screenshot in order to automatically correct the element recognition. ○ Visions: A feature which allows Customers to record End Users' actions on an application or website that it owns, controls, licenses or uses. Whenever a visitor visits Customer's website or application, Customer may collect via Visions™ information from such visitor regarding his or her use of that website or application, such as pages visited, links clicked, non-sensitive text entered (if Customer chooses to collect it), and mouse movements, as well as information more commonly collected such as masked IP address, referring URL, browser, operating system, cookie information, CSS animations and dynamic content ("Visitors' Information"). Visitors' Information, in the aggregate, may be considered as Personal Information as it may be linked to a user identifier or may include Personal Information. Visitors' Information may include: End User unique ID (stored in a cookie for tracking and may be stored on our servers), Visitors' clicks/touches on elements, changes to input field (like text fields, CSS selector or timestamp), elements and session meta-data, input on fields (depending on Customers settings), system errors, window size and changes to size, End User agent (browser, device), mouse position, page snapshot, whether a user clicked on a play or pause button of a video, and other events (scrolling, focusing, hiding pages etc.). Such information may identify the visitor. Visions™ uses masked IP addresses to determine End Users' geolocation (country and city in which you are located) to allow Customers to block recordings for certain End Users. By default, Visions™ does not record any keystrokes. This is the recommended setting, but can be changed via the settings page. Visions™ never records password inputs and provides the ability to specify that other elements of your website or application will not be tracked.
<p>Processing Activities; Business Purposes. The processing activities</p>	<p>Company's purposes of Processing are to facilitate its Services to Comcast, which are explained below:</p>

undertaken by the parties with respect to Personal Information.	<p><u>Passively Collected Information is collected in order to:</u></p> <ul style="list-style-type: none"> ○ Provide Customers with the Service; ○ For customization and improvement of the Service. <p><u>Personal Information is collected in order to:</u></p> <ul style="list-style-type: none"> ○ Provide Customers with the Service; ○ Contacting End Users and/or customers for the purpose of providing them with technical assistance and other related information about the Service; ○ Replying to End User's queries; ○ Troubleshooting problems, detecting and protecting against error, fraud or other criminal activity. ○ For risk control, to comply with laws and regulations, and to comply with other legal processes and law enforcement requirements. ○ To enforce agreements executed with WalkMe.
Recipients of Personal Information Transferred to the Data Importer	Data importer's (Company's) Subprocessors. See Exhibit I of the Agreement.
Data Subjects. The personal information transferred concern the following categories of data subjects.	<ul style="list-style-type: none"> • Comcast's customers • Comcast's employees
Special Categories of Data (if applicable)	<p>The following special categories of personal data may be included in the data Comcast.</p> <p>N/A</p> <ul style="list-style-type: none"> •
Purposes of the Transfer	To facilitate the Processing Activities described above.

Description of the technical and organisational security measures implemented by the data importer
Company will maintain security measures at least as protective as described below.

Overview of WalkMe's Technical and Organizational Security Measures

Certifications

WalkMe has and shall maintain, to the extent applicable, the following certifications:

- **ISO 27001:2013 Information Security Certification:** The ISO 27001:2013 audit (i) evaluates WalkMe's information security management system for the WalkMe's products, infrastructure and organization; and (ii) verifies that all information security controls are in place to ensure confidentiality, integrity and availability of personal information.

- **Skyhigh CloudTrust™: WalkMe was awarded the Skyhigh CloudTrust™ of Enterprise Ready™** by fulfilling a comprehensive set of requirements for data protection, identity verification, service security, business practices, and legal protection.
- **STAR Certification from the Cloud Security Alliance (CSA):** The STAR Certification is an internationally recognized cloud security certification program jointly developed by CSA and BSI that specifies comprehensive and stringent cloud security.
- **Service Organization Control Type II (SOC2):** The SOC 2 technical audit requires companies storing customer data in the cloud to establish and follow strict information security policies and procedures, encompassing the security, availability, processing, integrity, and confidentiality of customer data. SOC 2 ensures that a company's information security measures are in line with the unique parameters of today's cloud requirements.
- **Level 1 of Federal Information Process Standard 140-2 (FIPS 140-2):** FIPS 140-2 is a security standard for hardware, software and firmware solutions using cryptography in security systems that process sensitive and unclassified information.
- **EU-U.S. and Swiss-U.S. Certifications:** The EU-U.S. and Swiss-U.S. Privacy Shield frameworks provide companies with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States.
- **TrustArc (formerly TRUSTe) Certified Privacy and Third-Party Dispute Resolution Provider:** TrustArc validates the appropriateness and completeness of privacy policies and practices in accordance with applicable law and regulation, including EU-U.S. Privacy Shield requirements and provides third party dispute resolution services for the resolution of privacy and data use concerns.

Penetration Tests and Monitors

WalkMe's front and back-end applications and IT infrastructure undergo annual penetration tests completed by an independent third party. WalkMe utilizes the top-tier, secure, cloud services of Amazon Web Services (AWS). AWS undergoes its own independent periodic internal test and 24/7 monitoring of security-related events by the dedicated AWS security teams.

Access Control

WalkMe implements an integrated, comprehensive role-based user management and enforcement system. WalkMe must authorize any assigned roles to users and any permissions are controlled per action and screen with eight (8) roles built into WalkMe's Digital Adoption Platform (DAP) including, without limitation, administrator, content creator, publisher, analytics access, etc. Customer maintains the central management of deployment of the WalkMe DAP and can delegate usage and administrative permissions in its use of various elements and features of the WalkMe DAP.

Accountability and Security

WalkMe's corporate control access is centrally managed based on a strict need-to-know and least-privileged principles on all levels of the system:

- Applications (Strong Authentication);
- Network (Segmentation, Firewall);
- OS (Access To Services);
- Procedural (Authorized to Review/Approve Code, Manage Changes)

WalkMe's internal duties are segregated based on applicable duties between R&D (Code Development), Development Operations (Deployment), and Security (Security Controls). WalkMe conducts on a quarterly basis access review, including, without limitation, review of the firewall rules and user account permissions.

Furthermore, WalkMe has an extensive Security Information and Event Management System (SIEM) that collects security audit trail logs across infrastructure components in industry standard formats using an Intrusion Detection System.

**Appendix 2 to Data Processing Addendum:
Cross-border Transfer of Personal Information from the People's Republic of China to a Foreign
Country/Region**

1. The Parties' Roles

- 1.1. The parties agree that, for the purpose of this Appendix 2, Comcast (on behalf of its affiliates in China) is a data exporter and WalkMe is a data importer, regardless of their location.

For the purpose of this Appendix 2, the term "the People's Republic of China" or "China" does not include Hong Kong, Macao or Taiwan.

2. Personal Information to Be Transferred outside of China

- 2.1. For the purpose of this Agreement, Comcast will transfer certain Personal Information of the employees and contractors of Comcast's affiliates in China to WalkMe (collectively, "**China Employee Data**"). The types of China Employee Data include but are not limited to the information specified in Appendix 1a.
- 2.2. WalkMe agrees that, the China Employee Data received will only be Processed for the purpose of and in accordance with the Agreement. The China Employee Data will be retained by WalkMe for the specific length of period as stipulated in the Agreement, or if no such provisions in the Agreement the shortest and necessary periods to perform its Services under the Agreement. Upon termination or expiration of the Agreement, all China Employee Data must be destroyed or returned to Comcast in accordance with Section 8.6 of the Exhibit H-2 (Data Processing Addendum).
- 2.3. Except for the activities set forth in Appendix 1a, or unless otherwise allowed in the Agreement or Comcast agrees in writing, WalkMe shall not transfer any China Employee Data to any third parties (including but not limited to its affiliates and subcontractors). In addition, before WalkMe transfers any China Employee Data to any third parties, other than as permitted in Appendix 1a and the Agreement, the following conditions must be met:
- (i) WalkMe has, by means of, e-mail, instant messaging or letter, informed Comcast of the purposes of transferring China Employee Data to third parties by WalkMe, the identity and country of such third parties, the types of China Employee Data involved, and the periods for the storage of the China Employee Data by such third parties;
 - (ii) WalkMe has warranted that it will, when a data subject requests it to stop transferring the Personal Information to the third party, stop the transfer and instruct the third party to destroy or return the China Employee Data received; and
 - (iii) If any Personal Sensitive Information (as defined under the law of China) is involved, the consents from the data subjects have been obtained. For the avoidance of doubt, Comcast shall obtain from the applicable data subjects all the consents necessary for WalkMe to access or collect China Employee Data or Personal Information for purposes of delivering services to Comcast as set forth in Appendix 1a.

3. Rights of the Data Subjects

- 3.1. The parties acknowledge and agree that, the data subjects of the China Employee Data are the beneficiaries of relevant data protection provisions in the Agreement.
- 3.2. Comcast will, by e-mail, instant message, letter, fax, or other means, inform the data subjects of the basic information of itself and WalkMe, the purposes of the cross-border transfer of China Employee Data to WalkMe, relevant data types and the storage periods by WalkMe.

- 3.3. WalkMe agrees that if required by applicable laws, and if Comcast receives a request from the data subject for a copy of this Agreement or any part of it, Comcast shall promptly notify WalkMe before providing a copy of this Agreement or any part of it to such data subject, and Comcast shall redact the agreement and/or seek confidential treatment of the Agreement as reasonably permitted by applicable law.

Where the legitimate rights and interests of the data subjects of the China Employee Data are violated due to WalkMe's breach of this Agreement or applicable laws, WalkMe shall be liable to the data subjects for the losses of the data subjects.

4. Termination

- 4.1. WalkMe warrants and represents that, signing this Agreement and fulfilling the obligations thereunder will not breach the laws of the United States or any other applicable laws. If WalkMe becomes aware of any changes in the legal environment of the United States or elsewhere that may prevent its performance of this Agreement, WalkMe shall notify Comcast promptly and shall assist Comcast in reporting the same to the competent cyberspace administration authorities in China.
- 4.2. The parties agree that, if the changes of the legal environment in the United States or elsewhere make it impossible for WalkMe to perform the Agreement, Comcast has a right to, at its sole discretion, terminate this Agreement.
- 4.3. If the changes in the legal environment in the United States or elsewhere substantially interferes with WalkMe's ability to perform under the Agreement, Comcast may conduct a Personal Information protection security assessment(s) on WalkMe's Personal Information protection practice and such changes of legal environment for the purposes of determining relevant mitigation actions that WalkMe needs to take.
- 4.4. The parties agree that, if a competent cyberspace administration authority in China requires that the transfer of China Employee Data to WalkMe shall be suspended or ceased for any reason, the parties shall cooperate with each other to meet such requirements or, where allowed under applicable law, seek defences to such requirements.

Exhibit I

Approved Subcontractors

Entity Name	Location	Type of Services
Amazon Web Services Inc.	Seattle, Washington, U.S.A.	Hosting infrastructure services
Akamai Technologies Inc.	Cambridge, Massachusetts, U.S.A.	CDN + WAF services
Logz Hero Inc. (Logz.io)	Boston, U.S.A.	Logging services