BY EXECUTING THIS AGREEMENT IN WRITING, THE ORDERING ACTIVITY AGREES TO THE TERMS OF THIS END USER LICENSE AGREEMENT. IF ORDERING ACTIVITY IS ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR COMPANY OR OTHER LEGAL ENTITY, ORDERING ACTIVITY REPRESENTS AND WARRANTS THAT ORDERING ACTIVITY HAS FULL AUTHORITY TO BIND THAT PERSON, COMPANY OR LEGAL ENTITY TO THESE TERMS.

IF THE ORDERING ACTIVITY DOES NOT AGREE TO THESE TERMS, THEN DO NOT EXECUTE THIS AGREEMENT.

Definitions.

“Authorized Partner” means any of McAfee’s distributors, resellers or other business partners that are authorized by McAfee in writing to sell Support or the Software license rights granted under this Agreement.

“Cloud Services” means the cloud services that McAfee provides to Customer as specified in one or more Grant Letters. Access to the Cloud Services requires either an active support agreement or an active subscription, as required by the specific offering.

“Documentation” means explanatory materials in printed, electronic or online form accompanying the Software in English and other languages, if available.

“DATs” means detection definition files, also referred to as signature files, that contain the code(s) antimalware software uses to detect and repair viruses, Trojan horses, and potentially unwanted programs.

“Grant Letter” means a confirmation notice letter issued by McAfee to Ordering Activity, confirming the Software and Support purchased by Ordering Activity, including the applicable product entitlement, as defined in the Product Entitlement Definitions (further described at Section 3(a) below).

“High Risk System” means a device or system that requires extra safety functionalities such as fail-safe or fault-tolerant performance features to maintain a safe state where it is reasonably foreseeable that failure of the device or system could lead directly to death, personal injury, or catastrophic property damage. A device or system with a fail-safe feature in the event of failure may revert to a safe condition rather than break down, may include a secondary system that comes into operation to prevent a malfunction, or may operate as a backup in the event of a malfunction. A device or system with a fault-tolerant feature in the event of failure may continue its intended operation, possibly at a reduced level, rather than failing completely. Without limitation, High Risk Systems may be required in critical infrastructure, industrial plants, manufacturing facilities, direct life support devices, aircraft, train, boat
or vehicle navigation or communication systems, air traffic control, weapons systems, nuclear facilities,
power plants, medical systems and facilities, and transportation facilities.

“McAfee” means (i) McAfee, LLC, with offices located at 2821 Mission College Blvd., Santa Clara,
California 95054, USA, if the Software is purchased in the United States (except as provided in subclause
(vi), below), Canada, Mexico, Central America, South America, or the Caribbean, (ii) McAfee Ireland
Limited, with its registered offices located at Building 2000, City Gate, Mahon, Cork, Ireland, if the
Software is purchased in Europe, the Middle East, or Africa, (iii) McAfee (Singapore) Pte Ltd., with a
trading address located 101 Thomson Road 29-02/05 United Square, Singapore, 307591, Singapore, if
the Software is purchased in Asia (other than China (if the Software is purchased in RMB) or Japan) or
the region commonly referred to as Oceania, (iv) McAfee Co. Ltd., with offices located at Shibuya Mark
City West, 12-1, Dogenzaka 1-chome, Shibuya-ku, Tokyo, 150-0043, Japan, if the Software is purchased
in Japan, (v) McAfee (Beijing) Security Software Co. Ltd., with a trading address located at Room 616,
No. 6 North Workers’ Stadium Road, Chaoyang District, Beijing, China, if the Software is purchased in
China (in RMB), or (vi) McAfee Public Sector LLC, with offices located at 2821 Mission College Blvd.,
Santa Clara, California 95054, USA, if the Software is purchased by the U.S. Government, State or Local
Government, Healthcare organization or Educational institution within the United States.

“Software” means the McAfee software program in object code format (i) licensed from McAfee and
purchased from McAfee or its Authorized Partners, or (ii) embedded in or pre-loaded on McAfee-
branded hardware equipment purchased from McAfee or its Authorized Partners, in each case including
Upgrades and Updates that Ordering Activity install during the applicable Support period. Software may
also include additional features or functionality that can be accessed with either a current subscription
or active support contract to certain Cloud Services as required by the specific offering and subject to
the Cloud Terms of Service.

“Standard” means a technology specification created by a government sponsored group, an industry
sponsored group, or any similar group or entity that creates technology specifications to be used by
others. Examples of Standards include GSM, LTE, 5G, Wi-Fi, CDMA, MPEG, and HTML. Examples of
groups that create Standards include IEEE, ITU, 3GPP, and ETSI.

“Subsidiary” means any entity controlled by Ordering Activity through greater than fifty per cent (50%)
ownership of the voting securities.

“Support” or “Technical Support” means the support services offered by McAfee for the support and
maintenance of the Software and the McAfee-branded hardware equipment as further specified in the
McAfee Technical Support and Maintenance Terms.

“Updates” are related to content of the Software, including, without limitation, all DATs, signature sets,
policy updates, and database updates for the Software, and that are made generally available to
McAfee’s customer base as a part of purchased Support and which are not separately priced or
marketed by McAfee.

“Upgrade” means any and all improvements in the Software that are made generally available to
McAfee’s customer base as part of purchased Support and which are not separately priced or marketed
by McAfee.

License Grant; Proprietary Rights.
Subject to the terms and conditions of this Agreement, McAfee hereby grants to the Ordering Activity a nonexclusive, non-transferable right to use the Software (for the purpose of this Agreement, to use the Software includes to download, install, and access the Software) listed in the Grant Letter solely for the Ordering Activity’s own internal business operations. The Ordering Activity is not granted rights to Updates and Upgrades unless the Ordering Activity has purchased Support (or a service subscription granting rights to Updates and Upgrades).

The Software, including, without limitation, its object code and source code, whether or not provided to the Ordering Activity, is strictly confidential to McAfee. McAfee (or its licensors) owns exclusively and reserves all – and the Ordering Activity may not exercise any – right, title, and interest in and to the Software, including, without limitation, all intellectual property rights in and to the Software, except to the extent of the limited Software use license granted to the Ordering Activity in this Agreement. This Agreement is not an agreement of sale, and no title, intellectual property rights, or ownership rights to the Software are transferred to the Ordering Activity pursuant to this Agreement. You acknowledge and agree that the Software and all ideas, methods, algorithms, formulae, processes, and concepts used in developing or incorporated into the Software, all future Updates and Upgrades, and all other improvements, revisions, corrections, bug-fixes, hot-fixes, patches, modifications, enhancements, releases, DATs, signature sets, upgrades, and policy and database updates and other updates in, of, or to the Software, and all copies of the foregoing are trade secrets and proprietary property of McAfee, having great commercial value to McAfee. Ownership of derivative works should be as set forth in the copyright statute, 17 U.S.C. § 103 and the FAR clause at 52.227-14 (as applicable), but at a minimum, the Ordering Activity shall receive unlimited rights to use such derivative works at no further cost. Such rights shall not be construed as granting Ordering Activity any Software or Support (including Updates and Upgrades) at no charge.

All Cloud Services, and any Software that includes Cloud Services, are subject to the McAfee Cloud Terms of Service Agreement as an attached document to the GSA Schedule 70 contract.

Copy and Use Terms.

Product Entitlement: The use of the Software depends on the licenses purchased (e.g. nodes) and is subject to the Product Entitlement Definitions as an attached document to the GSA Schedule 70 contract on the applicable date of Ordering Activity’s Grant Letter.

Multiple Platforms/Bundles: If the Software supports multiple platforms or if the Ordering Activity receives the Software bundled with other software, the total number of devices on which all versions of the Software is installed may not exceed the Ordering Activity’s product entitlement. Certain Software licensed as part of a suite-based McAfee product may also require the purchase of a separate McAfee server license in order to use the Software on certain types of servers, in each case as specified in the Documentation.

Term: The license is effective for a limited period of time (“Term”) in the event that such Term is set forth in the Grant Letter, otherwise the licenses shall be perpetual.

Copies: The Ordering Activity may copy the Software as reasonably necessary for back-up, archival or disaster recovery purposes.
Subsidiaries; Managing Parties: The Ordering Activity may permit a third party with which Ordering Activity enters into a contract to manage Ordering Activity’s information technology resources (“Managing Party”), provided that (i) the Managing Party only uses the Software for Ordering Activity’s internal operations and not for the benefit of another third party or the Managing Party, (ii) the Managing Party agrees to comply with the terms and conditions of this Agreement and (iii) Ordering Activity provides McAfee with written notice that a Managing Party will be using the Software on Ordering Activity’s behalf. The Ordering Activity shall be responsible and fully liable for the Managing Party’s compliance with or breach of the terms of this Agreement.

General Restrictions: The Ordering Activity may not cause or allow any third party to: (i) decompile, disassemble or reverse-engineer the Software; or create or recreate the source code for the Software; (ii) remove, erase, obscure, or tamper with any copyright or any other product identification or proprietary rights notices, seal, or instructional label printed or stamped on, affixed to, or encoded or recorded in or on any Software or Documentation; or fail to preserve all copyright and other proprietary notices in all copies of the Software and Documentation made by Ordering Activity; (iii) lease, lend or use the Software for timesharing or service bureau purposes; sell, market, license, sublicense, distribute, or otherwise grant to any person or entity any right to use the Software except to the extent expressly permitted in this Agreement; or use the Software to provide, alone or in combination with any other product or service, any product or service to any person or entity, whether on a fee basis or otherwise; (iv) modify, adapt, tamper with, translate, or create derivative works of the Software or the Documentation; combine or merge any part of the Software or Documentation with or into any other software or documentation; or refer to or otherwise use the Software as part of any effort to develop software (including, without limitation, any routine, script, code, or program) having any functional attributes, visual expressions, or other features similar to those of the Software or to compete with McAfee; (v) except with McAfee’s prior written permission, publish any performance or benchmark tests or analysis relating to the Software; or (vi) attempt to do any of the foregoing. The Ordering Activity may not run or operate the Software in a cloud, Internet-based computing, or similar on-demand computing environment unless the Ordering Activity’s Grant Letter specifically provides such.

Technical Support and Maintenance.

The McAfee Technical Support and Maintenance Terms and Conditions apply if the Ordering Activity has purchased Support. The McAfee Technical Support and Maintenance Terms and Conditions are incorporated by reference and can be found as an attached document to the GSA Schedule 70 contract. After the support or service subscription period specified in a Grant Letter has expired, the Ordering Activity has no further rights to receive any Support including Upgrades, Updates and telephone support. The Ordering Activity will secure any and all privacy-related rights and permissions from individual persons as may be required by regulation, statute, or other law or Ordering Activity’s internal policies or guidelines in order to disclose to McAfee, in connection with McAfee’s performance of Support or otherwise under this Agreement, applicable personally identifiable information, data, and material.

Limited Warranty and Disclaimer.

Limited Warranty: McAfee warrants that, for a period of sixty (60) days from the purchase date (“Warranty Period”), the Software licensed hereunder will perform substantially in accordance with the Documentation (the
Limited Warranty).

Exclusive Remedy: In case of any breach of the above Limited Warranty, as Ordering Activity’s exclusive remedy and McAfee’s entire obligation and liability McAfee will (i) repair or replace the Software or (ii) if such repair or replacement would in McAfee’s opinion be commercially unreasonable, upon McAfee’s receipt of Ordering Activity’s written representation and promise that Ordering Activity has removed all instances of the Software and will not use the Software, refund the price paid by Ordering Activity for the applicable Software.

Exclusion of Warranty: THE ABOVE LIMITED WARRANTY WILL NOT APPLY IF: (i) THE SOFTWARE IS NOT USED IN ACCORDANCE WITH THIS AGREEMENT OR THE DOCUMENTATION, (ii) THE SOFTWARE OR ANY PART THEREOF HAS BEEN MODIFIED BY ANY ENTITY OTHER THAN MCAFEE OR (iii) A MALFUNCTION IN THE SOFTWARE HAS BEEN CAUSED BY ANY EQUIPMENT OR SOFTWARE NOT SUPPLIED BY MCAFEE.

Disclaimer: EXCEPT FOR THE LIMITED WARRANTY SET FORTH ABOVE, THE SOFTWARE IS PROVIDED “AS IS” AND MCAFEE MAKES NO REPRESENTATIONS OR WARRANTIES, AND MCAFEE DISCLAIMS ALL REPRESENTATIONS, WARRANTIES, AND CONDITIONS, ORAL OR WRITTEN, EXPRESS OR IMPLIED, ARISING FROM COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE IN TRADE, OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, OR SYSTEMS INTEGRATION. WITHOUT LIMITING THE FOREGOING, MCAFEE MAKES NO WARRANTY, REPRESENTATION, OR GUARANTEE AS TO THE SOFTWARE’S USE OR PERFORMANCE AND DOES NOT WARRANT, REPRESENT, OR GUARANTEE THAT THE OPERATION OF THE SOFTWARE WILL BE FAIL-SAFE, UNINTERRUPTED, OR FREE FROM ERRORS OR DEFECTS OR THAT THE SOFTWARE WILL PROTECT AGAINST ALL POSSIBLE THREATS.

High Risk Systems Terms: THE SOFTWARE MAY FAIL AND IS NOT DESIGNED, DEVELOPED, TESTED, OR INTENDED TO BE RELIABLE IN THE CONTEXT OF HIGH RISK SYSTEMS. WITHOUT LIMITING ANYTHING ELSE, MCAFEE HAS NO RESPONSIBILITY FOR ALL CLAIMS, SUITS, DEMANDS, AND PROCEEDINGS ALLEGING, CLAIMING, SEEKING, OR ASSERTING, ANY LIABILITY, LOSS, OBLIGATION, RISK, COST, DAMAGE, AWARD, PENALTY, SETTLEMENT, JUDGMENT, FINE, OR EXPENSES (INCLUDING ATTORNEYS FEES) ARISING FROM OR IN CONNECTION WITH ORDERING ACTIVITY’S USE OF THE SOFTWARE ON OR IN A HIGH RISK SYSTEM, INCLUDING, WITHOUT LIMITATION, THOSE THAT (i) COULD HAVE BEEN PREVENTED BY DEPLOYMENT OF FAIL-SAFE OR FAULT-TOLERANT FEATURES TO THE HIGH RISK SYSTEM, (ii) ARE BASED ON A CLAIM, ALLEGATION, OR ASSERTION THAT THE FUNCTIONING OF THE HIGH RISK SYSTEM DEPENDS OR DEPENDED ON THE FUNCTIONING OF THE SOFTWARE OR THAT THE FAILURE OF THE SOFTWARE CAUSED A HIGH RISK SYSTEM TO FAIL.

Limitation of Remedies and Damages.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, NEGLIGENCE, CONTRACT OR OTHERWISE, SHALL EITHER PARTY BE LIABLE TO THE OTHER UNDER THIS AGREEMENT OR IN CONNECTION WITH ITS SUBJECT MATTER FOR ANY INDIRECT, SPECIAL,
INCIDENTAL, PUNITIVE, EXEMPLARY, CONSEQUENTIAL, OR EXTRA-CONTRACTUAL DAMAGES OF ANY KIND, LOSS OF GOODWILL, LOSS OF PERSONNEL SALARIES, LOST PROFITS OR REVENUE, DAMAGES DUE TO WORK STOPPAGE AND/OR COMPUTER FAILURE OR MALFUNCTION, AND/OR COSTS OF PROCURING SUBSTITUTE SOFTWARE OR SERVICES, WHETHER OR NOT FORESEEABLE, EVEN IF THE EXCLUSIVE REMEDIES PROVIDED BY THIS AGREEMENT FAIL OF THEIR ESSENTIAL PURPOSE AND EVEN IF EITHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OR PROBABILITY OF SUCH DAMAGES.

REGARDLESS OF WHETHER THE CLAIM FOR SUCH DAMAGES IS BASED IN CONTRACT, TORT AND/OR ANY OTHER LEGAL THEORY, IN NO EVENT SHALL EITHER PARTY’S AGGREGATE LIABILITY TO THE OTHER PARTY FOR DIRECT DAMAGES UNDER THIS AGREEMENT OR IN CONNECTION WITH ITS SUBJECT MATTER EXCEED THE AMOUNT OF TOTAL FEES PAID OR PAYABLE BY THE ORDERING ACTIVITY FOR THE SOFTWARE GIVING RISE TO SUCH CLAIM.

No provision of this Agreement shall exclude or limit in any way (i) the liability of either party for death or personal injury caused by negligence or (ii) Ordering Activity’s liability for excess usage of and/or any breach of McAfee’s intellectual property rights in the Software.

THE LIMITATION OF LIABILITY IN THIS SECTION IS BASED ON THE FACT THAT END USERS USE THEIR COMPUTERS FOR DIFFERENT PURPOSES. THEREFORE, ONLY THE ORDERING ACTIVITY CAN IMPLEMENT BACK-UP PLANS AND SAFEGUARDS APPROPRIATE TO THE ORDERING ACTIVITY’S NEEDS IN THE EVENT THAT AN ERROR IN THE SOFTWARE CAUSES COMPUTER PROBLEMS AND RELATED DATA LOSSES. FOR THESE BUSINESS REASONS, THE ORDERING ACTIVITY AGREES TO THE LIMITATIONS OF LIABILITY IN THIS SECTION AND ACKNOWLEDGES THAT WITHOUT THE ORDERING ACTIVITY’S AGREEMENT TO THIS PROVISION, THE FEE CHARGED FOR THE SOFTWARE WOULD BE HIGHER.

THIS AGREEMENT SHALL NOT IMPAIR THE U.S. GOVERNMENT’S RIGHT TO RECOVER FOR FRAUD OR CRIMES ARISING OUT OF OR RELATED TO THIS CONTRACT UNDER ANY FEDERAL FRAUD STATUTE, INCLUDING THE FALSE CLAIMS ACT, 31 U.S.C. 3729-3733.

Intellectual Property Indemnity.

Indemnity: McAfee will indemnify, and, at its election, defend, the Ordering Activity against claims asserted against the Ordering Activity in a suit or action if: (i) the claim is for direct patent infringement or direct copyright infringement, or for McAfee’s trade secret misappropriation and (ii) the claim is (A) asserted against the Software, alone and not in combination with anything or (B) a combination of the Software.

Exclusions: Notwithstanding anything else in this Agreement, McAfee has no obligation to indemnify or defend the Ordering Activity for claims asserted, in whole or in part, against:

technology or designs that Ordering Activity gave to McAfee;

modifications or programming to Software that were made by anyone other than McAfee; or
the Software’s alleged implementation of some or all of a Standard.

Conditions: As a condition of McAfee’s obligations under this Section 7, the Ordering Activity must provide to McAfee: (i) prompt written notice of the claim and Ordering Activity’s agreement to give McAfee control over the defense and settlement of the claim; and (ii) the Ordering Activity’s full and timely good faith cooperation during the course of settlement negotiations and prosecution of the claim, and shall afford McAfee access to all nonprivileged communications and documentation with all parties, witnesses and judicial or administrative bodies associated with such claim upon McAfee’s request. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice’s right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

McAfee’s Consent: McAfee will not be responsible for any cost, expense, or compromise that the Ordering Activity makes or incurs without McAfee’s prior written consent.

Remedies: McAfee may, at its sole discretion and at is expense: (i) procure for the Ordering Activity the right to continue using the Software; (ii) replace the Software with a non-infringing Software; (iii) modify the Software so that it becomes non-infringing; or (iv) upon the Ordering Activity’s return of the Software to McAfee, and/or removal of the Software from Ordering Activity’s systems, refund the residual value of the purchase price paid by the Ordering Activity for the infringing Software, depreciated using a straight-line method of depreciation over a three (3) year period from the date of delivery of the Software to the Ordering Activity.

Personal Indemnity: The foregoing indemnity is personal to the Ordering Activity. The Ordering Activity may not transfer or to anyone, including Ordering Activity’s customers.

Exclusive Remedy: The indemnity section states McAfee’s entire obligation and the Ordering Activity’s exclusive remedy for claims of patent or copyright infringement, or trade secret misappropriation, made in whole or part against the Software.

Termination.

Without prejudice to the Ordering Activity’s payment obligations, the Ordering Activity may terminate the Ordering Activity’s license at any time by uninstalling the Software. Upon such termination, the Ordering Activity shall promptly return or destroy all copies of the Software and Documentation.

Additional Terms.

Evaluation Software: If the Software has been identified by McAfee as “Evaluation” Software, then the provisions of this section apply and shall supersede any other conflicting term of this Agreement. The Ordering Activity’s royalty-free, non-transferable, limited license to use the Evaluation Software, for evaluation purposes only, is limited to thirty (30) days unless otherwise agreed to in writing by McAfee. The Evaluation Software may contain errors or other problems that could cause system or other failures and data loss. Consequently, Evaluation Software is provided to the Ordering Activity “AS IS” and McAfee disclaims any warranty or liability obligations to the Ordering Activity of any kind. Support is not
available for Evaluation Software. Any information about the Evaluation Software gathered from its use shall be used solely for evaluation purposes and shall not be provided to any third parties. The restrictions described in Section 3(g) apply. If Ordering Activity fails to destroy the Evaluation Software after the evaluation period has expired, McAfee may address this in accordance with Section 14, Governing Law, of this agreement. WHERE LEGAL LIABILITY CANNOT BE

EXCLUDED, BUT MAY BE LIMITED, MCAFEE’S LIABILITY AND THAT OF ITS SUPPLIERS AND AUTHORIZED PARTNERS UNDER THIS AGREEMENT RELATED TO EVALUATION SOFTWARE, OR IN CONNECTION WITH EVALUATION SOFTWARE, SHALL BE LIMITED TO THE SUM OF FIFTY (50) U.S.

DOLLARS OR THE EQUIVALENT IN LOCAL CURRENCY IN TOTAL.

Beta Software: If the Software that the Ordering Activity has received has been identified by McAfee as “Beta” Software, then the provisions of Section 9(a) above shall apply accordingly. McAfee has no obligation to the Ordering Activity to further develop or publicly release the Beta Software. Support is not available for Beta Software. If requested by McAfee, Ordering Activity will provide feedback to McAfee regarding testing and use of the Beta Software, including error or bug reports. Ordering Activity agrees to grant McAfee a perpetual, nonexclusive, royalty-free, worldwide license to use, copy, distribute and make derivative works, and incorporate the feedback into any McAfee product at McAfee’s sole discretion. Upon receipt of a later unreleased version of the Beta Software or release by McAfee of a publicly released commercial version of the Beta Software, the Ordering Activity agrees to return or destroy all earlier Beta Software received from McAfee.

“Free” or “Open-Source” Software: The Software may include components (including, without limitation, programs, applications, tools, utilities, libraries, and other programming code) that are made available from third parties under a free or open source software licensing model (“FOSS Code”). FOSS Code components included with the Software are redistributed by McAfee under the terms of the applicable FOSS Code license for such component; the Ordering Activity receipt of FOSS Code components from McAfee under this Agreement neither enlarges nor curtails the Ordering Activity’s rights or obligations defined by the FOSS Code license applicable to the FOSS Code component. Copies of the FOSS Code licenses for FOSS Code components included with Software are included with or referenced in the Software’s Documentation. The Ordering Activity acknowledges, but does not agree to be bound, by such terms until they have been reviewed and agreed to in writing.

Notice to U.S. Government End Users.

The Software and accompanying Documentation are deemed to be “commercial computer software” and “commercial computer software documentation”, respectively, pursuant to FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

Privacy and Collection of Personal or System Information.

The Software, Support or service subscription may employ applications and tools to collect personally identifiable, sensitive or other information about Ordering Activity and users (e.g., including, without limitation, Ordering Activity’s and users’ name, address, e-mail address and payment details), their
computers, files stored on their computers, or their computers’ interactions with other computers (e.g., including, without limitation, information regarding network, licenses used, hardware type, model, hard disk size, CPU type, disk type, RAM size, 32 or 64 bit architecture, operating system types, versions, locale, BIOS version, BIOS model, total scanners deployed, database size, system telemetry, device ID, IP address, location, content, McAfee products installed, McAfee components, processes and services information, frequency and details of update of McAfee components, information about third party products installed, extracts of logs created by McAfee, usage patterns of McAfee products and specific features, etc.) (collectively, “Data”).

The collection of this Data may be necessary to provide the Ordering Activity and users with the relevant Software, Support or service subscription functionalities as ordered (e.g., including, without limitation, detecting and reporting threats and vulnerabilities on Ordering Activity’s and users’ computer network), to enable McAfee to improve our Software, Support or service subscription (e.g., including, without limitation, content synchronization, device tracking, troubleshooting, etc.), and to further or improve overall security for Ordering Activity and users. The Ordering Activity may be required to uninstall the Software or disable Support or its service subscription to stop further Data collection that supports these functions.

By entering into this Agreement, or using the Software, Support or service subscription, the Ordering Activity and users agree to the McAfee Privacy Policy as attached and to the collection, processing, copying, backup, storage, transfer and use of this Data by McAfee and its service providers, in, from and to the United States, Europe, or other countries or jurisdictions potentially outside of Ordering Activity’s or user’s own as part of the Software, Support or service subscription. McAfee will only collect, process, copy, backup, store, transfer and use personally identifiable information in accordance with the McAfee privacy policy as attached.

Audit.

Subject to applicable Government security requirements, upon thirty (30) days’ prior notice McAfee may request, and the Ordering Activity must provide, a Software-facilitated system-generated report (the “System Report”) verifying the Ordering Activity’s Software deployment. The Ordering Activity acknowledges that the System Report is based on technological features of the Software that provide Software deployment verification. If the Software does not contain technological features that provide Software deployment verification, the Ordering Activity will prepare and provide to McAfee within the thirty (30)-day period an accurate Software deployment verification report for the Software. McAfee will only request the System Report (or Ordering Activity’s prepared Software deployment verification report) one time per year and will not unreasonably interfere with the conduct of Ordering Activity’s business.

Export Controls.

The Ordering Activity acknowledges that the Software is subject to U.S. and when applicable, European Union export regulations. The Ordering Activity shall comply with applicable export and import laws and regulations for the jurisdiction in which the Software will be imported and/or exported. The Ordering
Activity shall not export the Software to any individual, entity or country prohibited by applicable law or regulation. The Ordering Activity is responsible, at Ordering Activity's own expense, for any local government permits, licenses or approvals required for importing and/or exporting the Software. For additional information regarding exporting and importing the Software, see “Export Compliance” as an attached document to the GSA Schedule 70 contract. If McAfee receives notice that Ordering Activity is or Ordering Activity becomes identified as a sanctioned or restricted party under applicable law, then McAfee will not be obligated to perform any of its obligations under this license if such performance would result in violation of the sanctions or restrictions.

Governing Law.

All disputes arising out of or relating to this Agreement or its subject matter will be governed by the substantive Federal laws of the United States of America. Specifically, any disputes relating to this Agreement shall be resolved in accordance with the FAR and the Contract Disputes Act, 41 U.S.C. §§ 7101-7109. This Agreement will not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. The Uniform Computer Information Transactions Act as enacted shall not apply.

Confidentiality

Each party hereto acknowledges that by reason of its relationship with the other party hereunder, it may have access to confidential information and materials concerning the other party’s business, technology, and/or products that is confidential to the other party (“Confidential Information”). Each party’s Confidential Information is of substantial value to the party, which value could be impaired if such information was disclosed to third parties or used in violation of this Agreement. Written or other tangible Confidential Information must at the time of disclosure be identified and labeled as Confidential Information belonging to the disclosing party. When disclosed orally or visually, Confidential Information must be identified as confidential at the time of the disclosure, with subsequent confirmation in writing within fifteen (15) days after disclosure. Each party agrees that it will not use in any way for its own account or the account of any third party, such Confidential Information, except as authorized under this Agreement, and will protect Confidential Information at least to the same extent as it protects its own Confidential Information and to the same extent that a reasonable person would protect such Confidential Information. Neither party may use the other party’s Confidential Information except to perform its duties or exercise its rights under this Agreement. The Confidential Information restrictions will not apply to Confidential Information that is (i) already known to the receiving party at the time of access hereunder, (ii) becomes publicly available through no wrongful act of the receiving party, (iii) independently developed by the receiving party without benefit of the disclosing party’s Confidential Information, (iv) has been rightfully received from a third party not under obligation of confidentiality or (v) is required to be disclosed by law, provided the party compelled to disclose the Confidential Information provides the party owning the Confidential Information with prior written notice of disclosure adequate for the owning party to take reasonable action to prevent such disclosure, where reasonably possible. Unless otherwise agreed to by both parties, upon termination of this Agreement or an applicable Addendum, each party will return the other party’s Confidential Information. This Agreement contains no confidential or proprietary information and shall be available to the public, provided however, that other items identified in this Agreement, including but not limited to source
code and other technical data, provided to Ordering Activity are Confidential Information and shall not be disclosed.

Miscellaneous.

Except for actions for non-payment or breach of McAfee’s proprietary rights in the Software and Documentation, no action, regardless of form, arising out of this Agreement may be brought by either party more than six (6) years after a party knew or should have known of the claim.

Any terms of this Agreement which by their nature should survive the termination of this Agreement shall survive such termination.

This Agreement together with the underlying negotiated Purchase Orders, represents the entire agreement between McAfee and the Ordering Activity and expressly supersedes and cancels any other communication, representation or advertising whether oral or written, on the subjects herein. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of McAfee and duly warranted Contracting Officer. However, this Agreement, including without limitation its termination, has no effect on any signed non-disclosure agreements between the parties, which remain in full force and effect as separate agreements according to their terms. The express provisions of this Agreement control over any course of performance, course of dealing, or usage of the trade inconsistent with any of the provisions of this Agreement. The provisions of this Agreement will prevail absent any agreed-upon, different, conflicting, or additional provisions that may appear on any Purchase Order, acknowledgment, invoice, or other writing issued by Customer in connection with this Agreement. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by McAfee. If any provision of this Agreement is held invalid, unenforceable, invalid, or prohibited under law, then such provision will be deemed restated to reflect the original intention of the parties as nearly as possible in accordance with applicable law and the remainder of this Agreement shall continue in full force and effect.

All notices, requests, demands and determinations for McAfee under this Agreement (other than routine operational communications) shall be sent to: the applicable entity address in Section 1(f) of this Agreement addressed to “Attention: Legal Department”.

MCAFEE TECHNICAL SUPPORT AND MAINTENANCE
TERMS AND CONDITIONS

McAfee will provide Technical Support services in accordance with the following terms and conditions (“Support Terms”). All capitalized terms not defined herein are defined in the applicable licensing or terms of service agreement.
Definitions.

“Authorized Partner” means any of McAfee’s authorized distributors, resellers or other business partners.

“Cloud Client Software” means Software that facilitates Ordering Activity’s access and use of the Cloud Services, and that does not perform functionality without active support or a subscription to the Cloud Services, and that does not perform functionality without active support or a subscription to the Cloud Services, as required by the specific offering. Cloud Client Software is provided as part of a subscription to Cloud Services, and may or may not necessarily be identified in a Grant Letter.

“Cloud Services” means the cloud services that McAfee provides to Ordering Activity as specified in one or more Grant Letters. Access to the Cloud Services requires either an active support agreement or an active subscription, as required by the specific offering.

“Ordering Activity” means the entity which has purchased Products and to which Intel provides Support.

“Grant Letter” means any written (electronic or otherwise) confirmation notice that Intel issues to Ordering Activity confirming Products and Support purchased by Ordering Activity, including without limitation Ordering Activity’s Support Level entitlement, the Grant Number, the Support Period and download details.

“Grant Number” means a unique number communicated by Intel in a Grant Letter confirming an Ordering Activity’s Support entitlement and is required when accessing Support.

“Hardware” means McAfee branded hardware equipment purchased from McAfee or its Authorized Partners, but excludes any Software or other intangible products.

“Product(s)” means McAfee’s Software and Hardware product specified in a Grant Letter or Cloud Services and Cloud Client Software purchased from McAfee or an Authorized Partner.

“Support”, “Technical Support” or “Technical Support and Maintenance” means the support services for McAfee Products purchased by Ordering Activity either from McAfee or from McAfee’s Authorized Partner which are dependent on the Support Level purchased.

“Software” means each McAfee software program in object code format and components licensed by McAfee or its Authorized Partners to Ordering Activity.

“Support Period” means the effective time period for which the Ordering Activity has purchased Support that is confirmed in a Grant Letter or in the case of Cloud Services means the effective time period for which the Ordering Activity has purchased the Cloud Services and has an active entitlement and valid account.

“Support Region” means any one of the following five (5) regions: (i) North America, (ii) Europe, Middle East and Africa (“EMEA”); (iii) Asia Pacific (“APAC”); (iv) Japan, and (v) Latin America (“LTAM”).

“Support Level(s)” means the McAfee Support offering purchased by Ordering Activity and defined at: https://support.mcafee.com/supportoptions.
“Upgrade” means any and all improvements in the Cloud Services or Software which are made generally available to McAfee’s customer base as a part of purchased Support and which are not separately priced or marketed by McAfee.

“Updates” means updates to the content of the Cloud Services or Software, and include without limitation all DATs (“DATs” or detection definition files, also referred to as signature files, are the code anti-malware software uses to detect and repair viruses, Trojan horses and potentially unwanted programs), signature sets, policy updates, database updates for the Cloud Services or Software which are made generally available to McAfee’s customer base as a part of purchased Support and which are not separately priced or marketed by McAfee.

Provision of Support. McAfee will provide Support to Ordering Activity during the Support Period at the Support Level that has been purchased by Ordering Activity and is confirmed to Ordering Activity in a Grant Letter or in the case of Cloud Services, based on the initial order or renewal. Ordering Activity will not be entitled to receive Support outside of the Support Period.

Updates and Upgrades. McAfee grants to Ordering Activity a non-exclusive, non-transferable license to use Upgrades and Updates provided by McAfee during the Support Period as a part of purchased Support. Such Upgrades and Updates are subject to the terms of the license granted by McAfee to the Ordering Activity for the Software. With the exception of Cloud Services, (a) Ordering Activity shall promptly download, distribute and install all Updates as released by McAfee during the Support Period and (b) McAfee strongly suggests that Ordering Activity also downloads, distributes and installs all Upgrades as released by McAfee during the Support Period. Ordering Activity acknowledges that any failure to do so could result in Ordering Activity’s inability to receive Updates and Technical Support and therefore could cause major security risks. An Upgrade may require a hardware upgrade or new platform conversion to function properly.

Supported Versions and End of Life. The provision of Support is limited to (a) the current version and (b) the immediately preceding version of the Product. Only the current version of Cloud Services will be supported. Notwithstanding any of the foregoing, Support is subject to McAfee’s End-of-Life Policy as an attached document to the GSA Schedule 70 contract. It is Ordering Activity’s responsibility to review McAfee’s Product Support Lifecycle webpage at:

Response Times. McAfee uses commercially reasonable efforts to meet the response times set forth in the escalation and response charters listed under https://support.mcafee.com/charters. Access to McAfee’s websites for the provision of Support may be suspended for brief periods due to scheduled maintenance and other factors.

Bug Fixing and Remote Diagnostics. McAfee uses commercially reasonable efforts to provide work-around solutions or patches to reported problems with Products. With Ordering Activity’s prior authorization, McAfee may perform remote diagnostics to work on reported problems. In the event Ordering Activity declines remote diagnostics, McAfee and Ordering Activity may agree to on-site Technical Support which is subject to an additional fee and reasonable travel and expenses, for which the Ordering Activity is responsible.

Support Period and Expired Support. The Support Period either begins (i) at the date the Product was purchased or (ii) at the renewal date of the expiration of a previous Support Period. Reinstating Out-of-Maintenance Support. If an Ordering Activity elects to terminate or allow its support services to lapse or expire, the Ordering Activity will be required to pay for the time that has lapsed since the end of such prior support services and the fees for the entire next annual period in accordance with the GSA Schedule Pricelist. Unless otherwise agreed upon by the parties, Support must be purchased within one (1) year after expiration of the previous Support period.

Support Coverage. Support is sold based upon the quantity of all Products purchased by Ordering Activity. Upon purchasing Support for a Product, Ordering Activity must purchase the same Support Level for all Product units owned, used or licensed by Ordering Activity that are deployed or in use at the location(s) covered by Support. Some Support Level(s) are available for purchase by Ordering Activity per Support Region.

Acquired Company Products. From time to time McAfee may acquire other companies and continue to support the products licensed or cloud services offered by such companies (“Acquired Products”). The Support Level(s) defined herein may not be applicable to the Acquired Products at the time of the acquisition but McAfee may within a reasonable period of time after the acquisition provide a description of the Support Level(s) available for the Acquired Products, which will become applicable once published on the Support webpage.

Exclusions. McAfee has no obligations to, (a) provide Support where hardware, tools or software other than those supplied or approved by McAfee have been incorporated with the Product (b) provide Support for Hardware damaged by or Hardware failures caused by Ordering Activity (c) import or export Ordering Activity data, create or modify custom business rules or reports, or support custom modifications to databases, active server pages, or other code, components or programs
(d) provide Support for problems that cannot be reproduced in running the Product in a configuration meeting published McAfee specifications or (e) provide Cloud Services Support for issues arising from any violation of the Cloud Services Agreement.

Obligations of Ordering Activity.

Support Process: Ordering Activity must report Product problems to McAfee Support organization, and be prepared to provide McAfee with (i) the Grant Number, (ii) the location of the Product, (iii) a detailed description of the problem, (iv) a description of the hardware on which the Software is loaded, including any serial number or service tag number where applicable, (v) the names and versions of any operating systems, networks, and software running with the Software, including patches and fixes, (vi) technical contact information and (vii) a detailed description of the problem. McAfee may request that Ordering Activity takes certain actions to determine whether the problem or error is related to the Product, or other item. Ordering Activity must reasonably cooperate with McAfee during this process.

Access: Ordering Activity shall provide McAfee with sufficient, free and safe access to the Products, Ordering Activity's computer systems networks and facilities in the event that it is agreed that McAfee will provide on-site support at Ordering Activity’s location or facilities or that McAfee will perform remote diagnostics. McAfee will conform to Ordering Activity’s security requirements before gaining access to Ordering Activity’s facilities, provided such requirements are issued in writing to McAfee reasonably prior to accessing such facilities.

Backup and Restore: Ordering Activity must keep adequate backup copies of data, databases, and application programs and agrees that Ordering Activity is solely responsible for any and all restoration and reconstruction of lost or altered files, data and programs.

Termination. Any terms which by their nature extend beyond the termination of this agreement remain in effect until fulfilled.

Hardware specific terms.

Region and Geographic Limitations: Unless otherwise agreed in writing by McAfee or included as part of the applicable Support Level, Hardware is eligible for service only if it remains in the country where Ordering Activity originally installed the Hardware. Geographic restrictions or limitations may apply to certain Hardware Support Levels and are described under https://support.mcafee.com/hardwarelocationmatrix (provided for informational purposes only).

Hardware Return: Prior to returning any Hardware to McAfee for repair or replacement, Ordering Activity must ensure that (i) the Hardware is free of any legal obligations or restrictions and of any Ordering Activity proprietary or confidential information that prevent McAfee from exchanging, repairing or replacing the Hardware, (ii) Ordering Activity has obtained a return authorization from McAfee, including a return material authorization number (a “RMA Number”). Hardware returned to
McAfee becomes the property of McAfee at the time it is received by McAfee and Ordering Activity shall assume ownership of all replacement Hardware provided by McAfee to Ordering Activity upon shipment by McAfee.

Restrictions: Ordering Activity must not, nor permit anyone else, to remove, alter, or obscure any proprietary notices or instructional labels on the Hardware without written authorization from McAfee. Ordering Activity must not install, nor permit the installation of additional hardware or software on the Hardware without written authorization from McAfee or breach any tamper seal on the Hardware.

Inspection Period: McAfee reserves the right to inspect Hardware for which Support has lapsed for more than ninety (90) days by itself or by its agents in consideration of a separate fee set forth in the Purchase Order and to request Ordering Activity to install the most current Upgrades and Updates before McAfee agrees to renew Support for the Hardware.

Resident Support Account Manager and Resident Product Specialist Terms.

If Ordering Activity purchases a Resident Support Account Manager (“RSAM”) or Resident Product Specialist (“RPS”), McAfee will provide an RSAM or RPS to provide on-site certain Support that Ordering Activity has purchased from McAfee. Additional information on the description and scope of the RSAM’s and RPS’s roles and responsibilities can be found at http://support.mcafee.com/documentation.

The RSAM or RPS will work during normal business hours as agreed upon between McAfee and Ordering Activity. The RSAM or RPS may be required to be out-of-the-office due to PTO, illness, holidays, training, vacations or meetings. During this time out-of-the-office, or should the RSAM’s or RPS’s employment with McAfee end, McAfee will provide to Ordering Activity the name and phone number of a temporary Support Account Manager (“SAM”) that will cover Ordering Activity’s account until the RSAM or RPS returns. The temporary SAM will provide Support services remotely.

Ordering Activity acknowledges and understands that the timeline to on-board at Ordering Activity’s location is approximately ninety (90) days from the time of the notification of the requirement. During this period, McAfee will assign an interim SAM to facilitate the Support services until the parties can agree upon the individual to be placed as an RSAM or RPS. McAfee and Ordering Activity will work together in good faith to select the RSAM or RPS. In the event Ordering Activity rejects the candidate or delays in the selection of a reasonable candidate McAfee has offered for consideration, McAfee will assign an interim SAM. For avoidance of doubt, the interim SAM will not be an on-site resource and may be a shared resource with other McAfee customers.

Ordering Activity acknowledges that McAfee employees are quickly deployed, and any delay in the selection of a candidate may: (1) result in Ordering Activity not being able to have its desired individual perform the Support services; (2) result in the use of an interim SAM (as stated above); and (3) hinder the performance of the Support services as described herein. Ordering Activity also acknowledges that it might not be possible to retain a particular individual for the duration of the term of the Support Period. The use of an interim SAM is, on its own, not sufficient to warrant a refund of fees or entitle Ordering Activity to service credits.
Malware Awareness Program Terms.

If, for the Support Period, Ordering Activity has purchased (1) Support for McAfee’s ePolicy Orchestrator Product (“ePO”), and (2) either (a) an RSAM, (b) an RPS, or (c) a Malware Awareness Program (“MAP”), as part of Support (as defined hereunder) McAfee will produce for Ordering Activity, once during the Support Period at a time agreed by Ordering Activity and McAfee, a MAP report in McAfee’s then-current standard form using data collected by McAfee through Ordering Activity’s deployment of ePO.

McAfee may change the standard form of the MAP report at McAfee’s discretion to reflect developments in malware and other security threats, information captured by ePO, or for other reasons identified by McAfee.

For the avoidance of doubt, (1) a license to ePO must be purchased separately by Ordering Activity in order for Ordering Activity to purchase Support for ePO, (2) a license to ePO is not included with Support, with the MAP report, or in connection with the MAP, but must be purchased separately by Ordering Activity, and (3) MAP is not included as part of Support unless Ordering Activity has separately purchased Support for ePO and has separately purchased an RSAM, an RPS, or MAP.

The MAP report and its contents, excluding Ordering Activity’s Confidential Information, are strictly confidential to McAfee, and, except to the extent expressed in the next sentence, McAfee owns and reserves all right, title, and interest therein and thereto. Upon delivery of the MAP report to Ordering Activity, McAfee grants to Ordering Activity a worldwide, royalty-free, perpetual, non-exclusive license under McAfee’s McAfee intellectual property rights to use and make a reasonable number of copies of the MAP report, in the form originally furnished by McAfee to Ordering Activity, for Ordering Activity’s own internal business purposes.

THE MAP AND MAP REPORTS ARE PROVIDED TO ORDERING ACTIVITY FOR ORDERING ACTIVITY’S INFORMATIONAL PURPOSES ONLY AND ON AN “AS IS” BASIS. MCAFEE DOES NOT REPRESENT OR WARRANT THAT MAP OR ANY MAP REPORT WILL IDENTIFY ALL MALWARE OR VULNERABILITIES. ANY OBSERVATIONS OR RECOMMENDATIONS GIVEN AS A PART OF MAP OR A MAP REPORT ARE GENERAL AND ARE NOT INTENDED AS SPECIFIC RECOMMENDATIONS OR COURSES OF ACTION. ORDERING ACTIVITY’S RELIANCE ON, ACTION ON OR LACK OF ACTION ON ANY SUCH OBSERVATIONS OR RECOMMENDATIONS IS AT ITS SOLE RISK.

OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING BUT NOT
LIMITED TO WARRANTIES OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY
QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT,
CONFORMITY TO ANY REPRESENTATION, SKILL AND CARE. MCAFEE DOES NOT WARRANT OR
GUARANTEE THAT SUPPORT WILL BE FREE FROM ERRORS OR DEFECTS OR THAT THE SUPPORT WILL
PROTECT AGAINST ALL POSSIBLE THREATS.

Some states or jurisdictions do not allow the exclusion of express or implied warranties, so the above
disclaimer may not apply to you. IN THAT EVENT SUCH EXPRESS OR IMPLIED WARRANTIES SHALL BE
LIMITED IN DURATION TO THE MINIMUM PERIOD REQUIRED BY THE APPLICABLE LAW (IF ANY).

Limitation of Liability; Confidentiality; Audit; Export Control. Ordering Activity agrees to these Technical
Support and Maintenance Terms and Conditions as part of one or more product licenses or services
agreements
between McAfee and the Ordering Activity (“Underlying Agreement”). THE LIMITATION OF LIABILITY,
CONFIDENTIALITY, PRIVACY, AUDIT AND EXPORT CONTROL PROVISIONS OF THE RELEVANT UNDERLYING
AGREEMENT ARE INCORPORATED INTO THESE TECHNICAL SUPPORT AND MAINTENANCE TERMS AND
CONDITIONS.

General.
Recording: In providing Support, McAfee may record all or part of telephone calls between
Ordering Activity and McAfee for quality assurance and training purposes in compliance with applicable
laws.

Assignment: The provision of Support is not assignable by Ordering Activity without the prior written
consent of McAfee. Any attempt of assignment by Ordering Activity without such consent will be void.
McAfee may subcontract its obligations to provide Support hereunder to another party, but with notice
to the Ordering Activity.

Governing law: All disputes arising out of or relating to this Agreement or its subject matter will be
governed by the Federal laws of the United States. This Agreement will not be governed by the United
Nations Convention on Contracts for the International Sale of Goods, the application of which is
expressly excluded. The Uniform Computer Information Transactions Act as enacted shall not apply.

Entire Agreement. The Support Terms and any additional terms referenced herein together with the
underlying negotiated Purchase Order(s), constitute the entire agreement between Ordering Activity
and McAfee with regard to Support, and supersedes all prior negotiations, agreements, and
understandings with respect to the subject matter hereof. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of McAfee and duly warranted Contracting Officer. However, this Agreement, including without limitation its termination, has no effect on any signed non-disclosure agreements between the parties, which remain in full force and effect as separate agreements according to their terms. The express provisions of this Agreement control over any course of performance, course of dealing, or usage of the trade inconsistent with any of the provisions of this Agreement. The provisions of this Agreement will prevail absent any agreed-upon, different, conflicting, or additional provisions that may appear on any purchase order, acknowledgment, invoice, or other writing issued by Customer in connection with this Agreement.

McAfee Cloud Services Agreement

McAfee, LLC. ("McAfee") and Customer (as identified in the Grant Letter) agree to the following McAfee Cloud Services Agreement ("Subscription Agreement"), the Supplemental Terms and Conditions set forth below or otherwise included with the pertinent Cloud Services or Software ("Supplemental Terms") and the terms as specified in the Grant Letter. If Customer does not agree to the terms in the Grant Letter, Customer should not execute this Subscription Agreement or the accompanying Purchase Order, and Customer must immediately notify McAfee to cancel the Cloud Services identified in the Grant Letter prior to accessing or using the Cloud Services or Software.

BY EXECUTING THIS SUBSCRIPTION AGREEMENT OR THE ACCOMPANYING GOVERNMENT PURCHASE ORDER

IN WRITING, YOU AGREE TO THE TERMS OF THIS AGREEMENT (INCLUDING THE APPLICABLE SUPPLEMENTAL TERMS AND GRANT LETTER) ON BEHALF OF CUSTOMER, AND YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND CUSTOMER TO THIS AGREEMENT.

1. DEFINITIONS. For purposes of the Agreement, the following definitions apply:

“Agreement” means this Subscription Agreement, the applicable Supplemental Terms, the Grant Letter.

“Annual Customers” means Customers who have a valid annual or multi-year contract for Cloud Services.

“Channel Partner” means the McAfee partner identified in the Grant Letter through which the Customer purchased the Cloud Services.

“Cloud Client Software” means Software that facilitates Customer’s access and use of the Cloud Services, and that does not perform functionality without active support or a subscription to the Cloud Services, as required by the specific offering. Cloud Client Software is provided as part of a subscription to Cloud Services, and may or may not necessarily be identified in a Grant Letter.

“Cloud Services” means the cloud services that McAfee provides to Customer as specified in one or more Grant Letters. Access to the Cloud Services requires either an active support agreement or an active subscription, as required by the specific offering.
“Control” means the possession of beneficial ownership of more than fifty percent (50%) of the voting power of the person or entity entitled to vote in the election of directors or, in the case of an entity that is not a corporation, the election of the corresponding managing authority.

“Customer Data” means any data provided by Customer to McAfee by and through the Software, Cloud Services, Support and any other products or services offered under this Agreement. Customer Data includes Personal Data as defined in Section 9 (Privacy).

“Documentation” means explanatory materials created by McAfee in printed, electronic or online form that accompany the Cloud Services or Software.

“Grant Letter” means any written (electronic or otherwise) confirmation notice that McAfee issues to Customer confirming the Licensed Product and Support purchased, License Period, and other access and use details. A Grant Letter includes a Welcome Letter or other purchasing documentation entered into between Customer and McAfee or Channel Partner for the Licensed Product.

“McAfee” means (i) McAfee, LLC, with offices located at 2821 Mission College Blvd., Santa Clara, California 95054, USA, if the Software is purchased in the United States (except as provided in subclause (vi), below), Canada, Mexico, Central America, South America, or the Caribbean, (ii) McAfee Ireland Limited, with its registered offices located at Pipers Way, Swindon, Wiltshire SN3 1NJ, United Kingdom, if the Software is purchased in Europe, the Middle East, or Africa, (iii) McAfee (Singapore) Pte Ltd., with a trading address located at 69/F, Central Plaza, 18 Harbour Road, Wanchai, Hong Kong, if the Software is purchased in Asia (other than China (if the Software is purchased in RMB) or Japan) or the region commonly referred to as Oceania, (iv) McAfee Co. Ltd., with offices located at Kokusai Building 5F, 1-1, Marunouchi 3-chome, Chiyoda-ku, Tokyo, 100-0005, Japan, if the Software is purchased in Japan, (v) McAfee (Beijing) Security Software Co. Ltd., with a trading address located at Room IIA/B, First Floor, No. 999 Ying Lun Road, Waigaoqiao Free Trade Zone, Pudong, Shanghai, 200131 China, if the Software is purchased in China (in RMB), or (vi) McAfee Public Sector LLC, with offices located at 2821 Mission College Blvd., Santa Clara, California 95054, USA, if the Software is purchased by the U.S. Government, State or Local Government, Healthcare organization or Educational institution within the United States.

“Intellectual Property Rights” means all intellectual property rights and industrial property rights (throughout the universe, in all media, now existing or created in the future, for all versions and elements, in all languages, and for the entire duration of such rights) arising under statutory or common law, contract, or otherwise, and whether or not perfected, including, without limitation, patent rights, copyrights, trade secret rights, and trademark rights.

“License Period” means, with respect to Cloud Services or Software, the time period for which Customer has purchased the right to receive the Cloud Services or Software, or, with respect to Cloud Client
Software, the time period for which Customer has purchased the right to receive Cloud Services that are accessed through the Cloud Client Software. The initial License Period is as specified in a Grant Letter.

“Licensed Product” means all Cloud Services, Software or Documentation to which Customer has rightful access through a valid Grant Letter.

"Malware" means applications, executable code, or malicious content that McAfee deems to be harmful.

“Monthly Customer” means Customers who have a valid monthly contract for Cloud Services with no annual or multi-year commitment.

"Node" means any kind of device capable of processing data and includes any of the following types of computer devices: diskless workstations, personal computer workstations, networked computer workstations, homeworker/teleworker home-based systems, file and print servers, e-mail servers, Internet gateway devices, storage area network servers (SANS), terminal servers and portable workstations connected or connecting to the server(s) or network. For Cloud Services, Node may also mean an instance of the specific Cloud Service or the number of Users or seats with access to the Cloud Services.

"Open Proxy" means an HTTP server that allows third-party relay or proxy of web traffic.

"Open Relay" means an SMTP Email server that allows third-party relay of Email messages.

"Software" means each McAfee software program in object-code format that is licensed from McAfee under this Agreement, including Updates and Upgrades, or any object-code delivered to Customer.

“Standard” means any generally recognized technology or technical standard promulgated, distributed, specified, or published by an entity whose activities include developing, coordinating, promulgating, amending, reissuing, or otherwise producing standardized technology specifications or protocols for adoption by product manufacturers or the public. “Standards” include “de facto” technology or technical standards that are initially introduced by one or more entities, which then become more widely adopted by others in other products; includes features characterized as “mandatory,” “optional,” and their equivalents; and includes versions characterized as “draft.”

"Subsidiary" refers to any entity Controlled by Customer, but only for so long as that Control exists.

“Support” means technical support provided as described in the then-current McAfee Technical Support and Maintenance Terms, which are attached hereto.

“Throughput” means the amount of data or files sent from the Customer through the Cloud Services.

“Updates” means updates to the content of the Cloud Services or Software, and include without limitation all DATs (“DATs” or detection definition files, also referred to as signature files, are the code anti-malware software uses to detect and repair viruses, Trojan horses and potentially unwanted programs), signature sets, policy updates, and database updates for the Cloud Services or Software, which are made generally available to McAfee’s customer base as a part of purchased Support and which are not separately priced or marketed by McAfee.
“Upgrades” means any and all improvements in the Cloud Services or Software which are made generally available to McAfee’s customer base as a part of purchased Support and which are not separately priced or marketed by McAfee.

“User” means a unique individual whom Customer has authorized to use the Cloud Services or Software pursuant to Customer’s license under this Agreement.

2. RIGHT OF USE AND RESTRICTIONS.

Right to Access and Use Cloud Services. Subject to the terms of this Agreement, McAfee grants Customer a nonexclusive, nontransferable, worldwide right to access and use the Cloud Services described in the Grant Letter, for up to the number of Users, Nodes, Throughput or other metering mechanism specified in the Grant Letter, solely for Customer’s internal business use during the License Period. Unless otherwise specified by McAfee, Cloud Services that are designed to be accessed through Software as provided by McAfee may be accessed only through such Software.

License to Install and use Cloud Client Software. Subject to the terms of this Agreement, McAfee grants Customer a nonexclusive, nontransferable, worldwide license to install and use the Cloud Client Software made available by McAfee to Customer in connection with the Cloud Services, for up to the number of copies specified in the Grant Letter, on equipment owned or operated by or on behalf of Customer, as needed to access and use the Cloud Services described in the Grant Letter, solely for Customer’s internal business use during the License Period. The Cloud Client Software is licensed, not sold, to Customer under the terms of this license. Customer may make a reasonable number of copies of the Cloud Client Software for back-up, archival, and disaster recovery purposes during the License Period. The Cloud Client Software must be de-installed and destroyed at the end of the License Period. If Customer enters into a contract in which a third party manages Customer’s information technology resources ("Managing Party"), Customer may enable such Managing Party to use the Cloud Client Software on Customer’s behalf, provided that (a) the Managing Party only uses the Cloud Client Software and Cloud Services for Customer’s internal operations; (b) the Managing Party agrees to be bound by the terms of this Agreement, (c) Customer provides McAfee with written notice that a Managing Party will be using the Cloud Client Software on Customer’s behalf, and (d) Customer remains responsible for all use of the Cloud Client Software and Cloud Services by the Managing Party.

Updates and Upgrades. Customer must have an active subscription to the Cloud Services, or have an active Support Agreement for the Cloud Services, as applicable, to receive Updates or Upgrades for the Cloud Services, Cloud Client Software, and any On-Premise Software.

User Licenses. User licenses cannot be shared or used by more than one individual User but may be reassigned to new Users who are replacing former Users that have been terminated or otherwise no longer use the Software or Cloud Services.

Subsidiaries. Customer may permit its Subsidiaries to use the Software and Cloud Services in accordance with the terms of this Agreement but only while the entity qualifies as Customer’s Subsidiary, and
provided that (i) each Subsidiary agrees to be bound by the terms of this Agreement, and (ii) Customer is responsible for each Subsidiary’s compliance with this Agreement.

Restrictions. Customer may not access or use the Software or Cloud Services if Customer is a direct competitor of McAfee, or for monitoring the availability, security, performance, functionality, or for any other benchmarking or competitive purposes without McAfee’s express written permission. Customer will not: (i) license, sublicense, sell, resell, transfer, assign, distribute, or otherwise commercially exploit or make the Software or Cloud Services available to any third party; (ii) use systems as an Open Proxy or Open Relay; (iii) modify, decompile, reverse engineer, or copy the Software or Cloud Services, or any of its components; (iv) use the Software or Cloud Services to conduct fraudulent activities; (v) attempt to gain unauthorized access to the Software or Cloud Services, engage in any denial of service attacks, or otherwise cause immediate, material or ongoing harm to McAfee, its provision of the Software or Cloud Services, or others; (vi) impersonate or misrepresent an affiliation with a person or entity; (vii) use the Software or Cloud Services to initiate or propagate Malware; (viii) use the Software or Cloud Services for any purpose that violates applicable law or regulation, infringes on the rights of any person or entity, or violates this Agreement; (each of (i) to (viii), a "Prohibited Use").

Reserved Rights. The Cloud Services and Software, including, without limitation, their object code and source code, whether or not provided to Customer, are strictly confidential to McAfee. McAfee (or its licensors) owns exclusively and reserves all rights to the Cloud Services and Software, and Customer may not exercise any, right, title, and interest in and to the Cloud Services or Software, including, without limitation, all Intellectual Property Rights in and to the Cloud Services or Software, except to the extent of the limited rights and licenses granted to Customer in this Agreement. This Agreement is not an agreement of sale, and no title, Intellectual Property Rights, or ownership rights to the Cloud Services or Software are transferred to Customer pursuant to this Agreement. Customer acknowledges and agrees that the Cloud Services and Software and all ideas, methods, algorithms, formulae, processes, and concepts used in developing or incorporated into the Cloud Services and Software, all future Updates and Upgrades, and all other improvements, revisions, corrections, bug-fixes, hot-fixes, patches, modifications, enhancements, releases, DATs, signature sets, upgrades, and policy, database, and other updates in, of, or to the Cloud Services or Software, all derivative works based upon any of the foregoing, and all copies of the foregoing are trade secrets and reserved to and proprietary property of McAfee.

Right to Use Customer Data. Customer hereby grants McAfee a limited, non-exclusive, royalty-free, license to access and use the Customer Data as necessary for (i) McAfee to provide the Software, Cloud Services and technical support to Customer during the applicable License Period; (ii) to maintain or improve the Cloud Services and Software and other security related products, including to develop Updates and Upgrades; (iii) for internal research for threat protection solutions, such as improved spam protection (unless Customer opts out of such uses through the options available in the console); (iv) for administration of the Agreement, and (v) for purposes set forth in McAfee’s Privacy policies available at http://www.mcafee.com/common/privacy/english/. In addition, Customer acknowledges and agrees to the use or sharing by McAfee of aggregated, anonymized or pseudonomized Customer Data (such that it no longer identifies Customer or any individual) as a part of a larger set of statistics (for example, statistics describing the enterprise, amount of traffic, success rates, and the like) and that such data does not constitute Confidential Information.
Open Source Software. Customer acknowledges that the Software may include components (including, without limitation, programs, applications, tools, utilities, libraries, and other programming code) that are made available from third parties under a free or open source software licensing model (“FOSS Code”). FOSS Code components included with the Software are redistributed by McAfee to Customer under the terms of the applicable FOSS Code license for such component, and Customer’s receipt of FOSS Code components from McAfee under this Agreement neither enlarges nor curtails Customer’s rights or obligations defined by the FOSS Code license applicable to the FOSS Code component. Copies of the FOSS Code licenses for FOSS Code components included with Software are included with the Software or its Documentation.

3. BETA RELEASES AND EVALUATIONS. If Customer has signed up for an evaluation of Software or Cloud Services (“Evaluation Product”), or is given access to Software or Cloud Services identified as not generally available for commercial use, such as “Beta” or “Pre-Release” (“Beta Product”), then the provisions of this Section shall apply and shall control over any other conflicting terms of this Agreement. Customer’s use of an Evaluation Product is limited to thirty (30) days unless otherwise agreed to in writing by McAfee, during which time Customer may access and use the Evaluation Product solely for Customer’s internal evaluation to decide whether to purchase the right to use the Evaluation Product. McAfee reserves the right to materially change or discontinue Beta Products at any time and without notice to Customer. Access or use of a Beta Product is restricted to Customer’s internal performance evaluation of the Beta Product. McAfee is not obligated to finally release any version of the Beta Product. Customer will report to McAfee unusual, unplanned, or out of the ordinary events observed in a Beta Product. McAfee has no obligation to provide any Support for Evaluation Products or Beta Products. Customer acknowledges that the Evaluation Products and Beta Products may contain errors, defects or other problems that could cause system or other failures, security breaches, interruptions and data loss. CONSEQUENTLY, EVALUATION PRODUCTS AND BETA PRODUCTS ARE PROVIDED TO CUSTOMER SOLELY ON AN “AS IS” BASIS, AND MCAFEE DISCLAIMS ALL WARRANTIES AND LIABILITY IN CONNECTION WITH THE EVALUATION PRODUCTS AND BETA PRODUCTS.

CUSTOMER ASSUMES ALL RISK OF USE OF EVALUATION PRODUCTS AND BETA PRODUCTS. WHERE LEGAL LIABILITY CANNOT BE EXCLUDED, BUT MAY BE LIMITED, THE AGGREGATE LIABILITY OF MCAFEE AND LICENSORS SHALL BE LIMITED TO THE SUM OF FIFTY (50) UNITED STATES DOLLARS (OR THE THEN-CURRENT VALUE IN THE RELEVANT LOCAL CURRENCY) IN TOTAL.

CUSTOMER OBLIGATIONS

Customer is responsible for all activity occurring under Customer’s Software, Cloud Services and Support accounts. Customer will provide McAfee with all information and assistance required to supply the Software or Cloud Services or enable Customer’s use of the same. Customer will immediately notify McAfee of any: (i) unauthorized account use or other suspected security breach; (ii) unauthorized use, copying or distribution of Software, Documentation or Customer Data; and (iii) unusual performance of the Software or Cloud Services observed by Customer.
Customer must obtain all necessary rights and permissions from Users. Customer represents and warrants that: (i) Customer has the legal rights and applicable consents to provide Customer Data to McAfee, (ii) Customer will comply with all applicable laws for processing and transferring Customer Data to McAfee and (iii) Customer retains adequate back-ups of Customer Data. Customer has sole responsibility for the accuracy, quality, integrity, legality, reliability, and appropriateness of all Customer Data. The Cloud Services rely on Customer Data as supplied by Customer, and McAfee is not liable for the content of Customer Data. McAfee does not assume any duty or obligation to correct or modify Customer Data.

As needed, Customer will provide McAfee contact information for Customer’s system administrator, who is authorized to provide the information required to configure and manage the Cloud Services (“System Administrator”). Depending on the Cloud Services purchased, McAfee may provide Customer with a confidential access code to the administration tool, which may only be accessed by the System Administrator.

Customer agrees to provide current and complete account Users’ information as necessary for McAfee to manage Customer’s account. Customer agrees to accept McAfee emails relevant to Customer’s receipt of the Cloud Services at the e-mail address specified by its System Administrator.

Customer agrees that McAfee may rely on all information provided to McAfee by the Customer. McAfee may provide all notices, statements, and other communications arising under this Agreement (other than legal notices) to Customer through either e-mail, posting on the Cloud Services or other electronic transmission.

TECHNICAL SUPPORT SERVICE. The McAfee Technical Support and Maintenance Terms apply to the Software and Cloud Services. The McAfee Technical Support and Maintenance Term are attached hereto below.

TERM; TERMINATION; LICENSE PERIODS.

Term. The term of this Agreement will continue until the termination of all License Periods, unless terminated sooner in accordance with this Agreement.

Termination.

When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be made as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, McAfee shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

Pursuant to FAR 52.233-1, upon termination of this Agreement, all License Periods will terminate. After the termination of the License Period for a particular Service, Customer agrees that McAfee has no obligation to retain Customer Data for that Service, which may be irretrievably deleted as part of McAfee’s record and information management and in accordance with applicable laws. To the extent any Customer Data is stored by the Service, Customer is solely responsible for retrieving that Customer Data.
License Periods. The initial License Period for each of the Cloud Services (including any Cloud Client Software used to access the Cloud Services) or for any other Software is specified in the Grant Letter (the "Initial License Period").

End-of-Life. McAfee’s provision of the Cloud Services and Software is subject to McAfee’s End-of-Life Policy attached hereto. Upon the End of Life date of the Cloud Services (as described in the End-of-Life Policy), the License Period for the Cloud Services (including Cloud Client Software used to access the Cloud Services) will terminate.

Suspension of Service. McAfee may suspend the Cloud Services: (a) if McAfee deems it necessary to prevent or terminate any actual or suspected Prohibited Use; or (b) upon notice to Customer if: (i) Customer commits a material breach of this Agreement; (ii) if McAfee receives notice from Channel Partner that Customer is in material breach of the Agreement, (iii) McAfee determines that the volume of data being transmitted or processed through the Cloud Services under Customer’s account is significantly greater than the average use or may cause degradation of the Cloud Services for Customer or other customers; or (iv) in the event of a threat to the security and integrity of the hosted environment and/or Customer Data. McAfee may temporarily suspend the Cloud Services if McAfee determines that the volume of data transmitted or processed through the Cloud Services under Customer’s account causes a degradation of the services. Temporary suspension of Cloud Services shall be without prejudice to any rights or liabilities accruing prior to or during the suspension, including Customer’s obligation to pay fees.

Survival. Sections 1, 6-11, 13-18 and 20-29 will survive the termination (including by expiration) of this Agreement.

PAYMENTS; TAXES; AUDIT.

Payments. Unless Customer is purchasing the Licensed Products through a Channel Partner, in which case payment obligations shall flow exclusively between Channel Partner and Customer, Customer will pay McAfee the fees set forth in the Grant Letter within thirty (30) days of the invoice date.

Transaction Taxes. Customer will pay all applicable transaction taxes, including, but not limited to, sales and use taxes, value added taxes, duties, customs, tariffs, and other government-imposed transactional charges however designated (and any related interest or penalty) on amounts payable by Customer under this Agreement ("Transaction Taxes"). Unless Customer is purchasing the Licensed Products through a Channel Partner, in which case obligations regarding Transaction Taxes shall be exclusively the responsibility of Channel Partner and Customer, McAfee will separately state on its invoices the Transaction Taxes that McAfee is required to collect from Customer under applicable law. Customer will provide proof of any exemption from Transaction Taxes to McAfee at least 15 business days prior to the due date for paying an invoice. If McAfee does not collect the required Transaction Taxes from Customer but is later required to remit such Transaction Taxes to any taxing authority, Customer will promptly reimburse McAfee for such Transaction Taxes, including any accrued penalty or interest charges if the failure to timely collect and remit was not due to the fault of McAfee. McAfee shall state separately on invoices taxes excluded from...
the fees, and Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with FAR 52.229-1 and FAR 52.229-3.

Withholding Taxes. All payments due from Customer will be made free and clear without deduction for any present and future taxes imposed by any taxing authority. Unless Customer is purchasing the Licensed Products through a Channel Partner, in which case obligations regarding Withholding Taxes (as defined below) shall be exclusively the responsibility of Channel Partner and Customer, if Customer is required by applicable law to deduct or withhold income taxes from amounts payable to McAfee under this Agreement (“Withholding Taxes”), Customer will remit, and provide McAfee with evidence that Customer has remitted, the Withholding Taxes to the appropriate taxing authority and pay to McAfee the remaining net amount. Customer will provide written notice to McAfee of its intent to withhold (including details of the amounts and legal basis for the Withholding Taxes) at least 15 business days prior to the due date for any payments under this Agreement and will cooperate with McAfee to reduce any Withholding Taxes. If McAfee provides Customer with valid and official documentation issued by the relevant taxing authority for a lower rate of Withholding Taxes, then Customer will apply the lower rate.

Income Taxes. Each party is responsible for its own income taxes or taxes based on gross revenues or gross receipts.

Audit. McAfee has the right, at its expense, to audit Customer’s compliance with the terms of this Agreement, and Customer will provide all records and information reasonably necessary for McAfee to successfully perform such audit. Such audit shall be conducted in a manner consistent with Government security requirements. If any audit reveals that Customer owes fees to McAfee, or the Channel Partner, McAfee or Channel Partner shall invoice Customer for such underpaid amounts. Customer consents to McAfee’s disclosure of such audit results to the Channel Partner.

CONFIDENTIALITY. In connection with this Agreement, each party may receive or have access to confidential information and materials of the other party. As used in this Agreement, “Confidential Information” means information that (a) is designated as “confidential” or by similar words by the disclosing party at the time of disclosure and, if oral or visual, is confirmed as confidential by the disclosing party in writing within 15 days of disclosure; or (b) the receiving party should reasonably have considered to be confidential under the circumstances surrounding disclosure; but Confidential Information does not include any information that (i) was previously known to the receiving party, (ii) is received from a third party without similar restriction, (iii) is or becomes publicly available other than through unauthorized disclosure, or (iv) is independently developed by the receiving party without the use of the other party’s Confidential Information. Customer acknowledges that McAfee’s Cloud Services access codes and nonpublic information regarding the Licensed Products and McAfee’s Intellectual Property Rights are McAfee’s Confidential Information. As between the parties, the disclosing party owns the Confidential Information it discloses to the receiving party. Each party will take reasonable precautions (at least as great as the precautions it takes to protect its own confidential information) to prevent unauthorized use or disclosure of the other party’s Confidential Information in its possession. Neither party will (a) disclose any Confidential Information of the other party to any third party during the term of this Agreement and for as long thereafter as the Confidential Information remains competitively sensitive, but not in any event for less than 7 years following the termination of this Agreement, or (b) use any Confidential Information of the other party except in the performance of its
obligations or exercise of its rights under this Agreement; but a party may disclose Confidential Information of the other party (i) to its employees, contractors or agents, on a need-to-know basis, under an obligation of confidentiality no less stringent than that set forth in this Section, and (ii) as required by law, provided that the receiving party notifies the disclosing party as soon as feasible and cooperates with the disclosing party’s efforts to limit or avoid the disclosure. McAfee recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which requires that certain information be released, despite being characterized as “confidential” by the vendor.

DATA PROTECTION. The Software, Cloud Services or Support may employ applications and tools to collect Customer Data that includes one or more data elements that can be used to identify a natural person ("Personal Data"). For the purpose of the Agreement, with respect to Personal Data, Customer and McAfee acknowledge that McAfee is a Data Processor and Customer is a Data Controller.

In accordance with the instructions provided by Customer through one or more orders under this Agreement, McAfee will collect, process, copy, backup, store, transfer and use (collectively “Process”) Personal Data. Processing may take place in, from and to the United States, Europe, or other countries or jurisdictions, potentially outside of the Customer or User’s own.

For Personal Data originating from Customer (for the purposes of the Standard Contractual Clauses the "Data Exporter") established in the European Economic Area and Switzerland (an “EU Transfer”) the Standard Contractual Clauses will apply to the Processing by McAfee outside of the European Economic Area (who, for the purposes of the Standard Contractual Clauses shall be deemed the “Data Importer”). “Standard Contractual Clauses” mean the standard contractual clauses for the transfer of Personal Data from a Data Controller in the European Economic Area to Processors established in third countries under the EU Data Protection Directive 95/46/EC (the "Directive") or any legislation replacing the Directive, (or any alternative or successor Decision that approves new standard contractual clauses for transfers to Data Processors in third countries). The Standard Contractual Clauses are available on the European Commission's website at the following link: Standard Contractual Clauses. The Standard Contractual Clauses will cease to apply if McAfee is certified under the EU/US Privacy Shield or if McAfee adopts Processor Binding Corporate Rules or an alternative recognized compliance standard for the lawful transfer of Personal Data (as defined in the Directive) outside the European Economic Area upon notice hereof by McAfee to Customer. If there is any conflict between the Standard Contractual Clauses and this Agreement, the Standard Contractual Clauses shall prevail. Customer is solely responsible for securing any privacy-related rights and permissions from individual persons and third parties as required by regulation, statute, or other law, or by Customer’s internal policies or guidelines, in order to use the Licensed Products or disclose to McAfee any personally identifiable information.

Where required in support of the permitted uses under this Agreement, Personal Data may be shared with third parties, including vendors, suppliers and partners ("Sub-Processors"). McAfee will restrict Sub-Processors access to Personal Data to the extent needed for performance and will impose written contractual obligations that are no less protective of the Personal Data than those obligations set forth in this Agreement.
McAfee may use cookies to store user session information, access codes and application settings to ease site navigation processes. McAfee will implement technical, organizational and administrative security measures in order to protect the Personal Data it Processes from unauthorized access and misuse while under McAfee’s custody or control. McAfee restricts its personnel from Processing Personal Data without authorization and will impose appropriate obligations upon its personnel, regarding confidentiality, data protection and data security. McAfee will not disclose Personal Data to any third party (including any government agency, court, or law enforcement agency) except with written consent from Customer or as necessary to comply with the law or valid legal process (e.g., subpoena, warrant, or court order). If a third party makes a request to McAfee for access to or correction of Personal Data, McAfee will refuse such request and instruct the third party to request that Personal Data directly from Customer and provide the third party with Customer’s contact information. If compelled to disclose Personal Data to a law enforcement agency or a third party, McAfee will endeavor to give Customer reasonable notice of the access request prior to granting such access, to allow Customer to seek a protective order or other appropriate remedy. If such notice is legally prohibited, McAfee shall take reasonable measures to protect the Personal Data from undue disclosure, as if it were McAfee’s own Confidential Information being requested. McAfee will notify Customer without undue delay if it becomes aware of unauthorized access or misuse of the Personal Data it Processes under this Agreement and will take reasonable steps to mitigate the effects and to minimize any resulting damage.

INTELLECTUAL PROPERTY. The Licensed Products are the sole and exclusive property of McAfee or its licensors, who retain sole ownership of all right, title and interest in Licensed Products, as well as any derivative works thereof. These ownership rights include all Intellectual Property Rights. Customer agrees, on behalf of itself and its Subsidiaries, that Customer and its Subsidiaries will take no action inconsistent with McAfee’s Intellectual Property Rights. Customer agrees that McAfee has the unrestricted right to use suggestions and feedback provided by Customer regarding products and services of McAfee and its affiliates, without notice to, payment to or consent from Customer, and that Customer will treat such suggestions and feedback as the Confidential Information of McAfee, and not Customer. Customer retains all right, title and interest in and to Customer Data.

LIMITED WARRANTY, REMEDIES AND DISCLAIMERS.

LIMITED WARRANTY. McAfee warrants that the Cloud Services will perform substantially in accordance with its Documentation. This warranty is personal to Customer and may not be assigned, transferred or passed-through to any third party.

THIS WARRANTY WILL NOT APPLY IF (i) THE CLOUD SERVICES OR SOFTWARE IS NOT USED IN ACCORDANCE WITH THIS AGREEMENT OR ITS DOCUMENTATION; (ii) THE SOFTWARE HAS BEEN MODIFIED BY ANY PERSON OR ENTITY OTHER THAN MCAFEE; OR (iii) A MALFUNCTION IN THE CLOUD SERVICES OR SOFTWARE HAS BEEN CAUSED BY ANY SYSTEMS, EQUIPMENT OR TECHNOLOGY NOT SUPPLIED BY MCAFEE.
LIMITATION OF REMEDY. The sole and exclusive remedy, and McAfee’s entire obligation and liability, for McAfee’s breach of warranty under this Agreement is for McAfee to repair or replace the Cloud Services to conform with its Documentation. If McAfee is unable to do so, McAfee may, in its own discretion, allow Customer to terminate the Agreement immediately upon notice to McAfee. In such event, if Customer paid fees directly to McAfee and not to a Channel Partner, McAfee will provide to Customer a pro-rata refund of the fees paid under this Agreement for the remainder of the then-current monthly or annual term.

EXCLUSIONS; DISCLAIMERS.

EXCEPT FOR THE LIMITED WARRANTY IN SECTION 11(a) (Limited Warranty), ALL LICENSED PRODUCTS, SUPPORT, AND OTHER ITEMS ARE PROVIDED TO CUSTOMER “AS IS” AND “WITH ALL FAULTS” AND MCAFEE MAKES NO REPRESENTATIONS OR WARRANTIES, AND DISCLAIMS ALL REPRESENTATIONS, WARRANTIES, AND CONDITIONS, ORAL OR WRITTEN, EXPRESS OR IMPLIED, ARISING FROM COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE IN TRADE, OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, OR SYSTEMS INTEGRATION.

WITHOUT LIMITATION, MCAFEE DOES NOT REPRESENT OR WARRANT ANY OF THE FOLLOWING: (i) THAT ANY LICENSED PRODUCT, DEVICE, NETWORK, SUPPORT, OR SYSTEM WILL OPERATE UNINTERRUPTED OR BE FAILSAFE OR ERROR-FREE; (ii) THAT ANY LICENSED PRODUCT, DEVICE, ADVICE, REPORT, OR DATA, WILL BE FREE FROM ERRORS OR COMPLY WITH ANY PARTICULAR LAW; (iii) ANY BUSINESS RESULTS CUSTOMER MAY ACHIEVE; (iv) THAT ANY OR ALL SYSTEM VULNERABILITIES OR WEAKNESSES WILL BE DISCOVERED; OR (v) COMPLETE PROTECTION AGAINST ANY SECURITY THREATS OR OTHER POSSIBLE RISKS.

CUSTOMER WILL NOT MAKE ANY REPRESENTATION OR OTHER STATEMENT OR UNDERTAKE ANY ACT OR OMISSION INCONSISTENT WITH THIS SECTION 11(c) (Exclusions; Disclaimers).

THE LICENSED PRODUCTS MAY FAIL AND ARE NOT DESIGNED, DEVELOPED, TESTED, OR INTENDED TO BE RELIABLE IN THE CONTEXT OF HIGH RISK SYSTEMS.

MCAFEE HAS NO RESPONSIBILITY FOR ALL CLAIMS, SUITS, DEMANDS, AND PROCEEDINGS ALLEGING, CLAIMING, SEEKING, OR ASSERTING, ANY LIABILITY, LOSS, OBLIGATION, RISK, COST, DAMAGE, AWARD, PENALTY, SETTLEMENT,
JUDGMENT, FINE, OR EXPENSES (INCLUDING ATTORNEYS’ FEES) ARISING FROM
OR IN CONNECTION WITH CUSTOMER’S USE OF THE PRODUCTS ON OR IN A HIGH
RISK SYSTEM, INCLUDING, WITHOUT LIMITATION, THOSE THAT (a) COULD HAVE
BEEN PREVENTED BY DEPLOYMENT OF FAIL-SAFE OR FAULT-TOLERANT
FEATURES TO THE HIGH RISK SYSTEM, OR
(b) ARE BASED ON A CLAIM, ALLEGATION, OR ASSERTION THAT THE
FUNCTIONING OF THE HIGH RISK SYSTEM DEPENDS OR DEPENDED ON THE
FUNCTIONING OF THE PRODUCTS OR THAT THE FAILURE OF ANY PRODUCT CAUSED A HIGH RISK
SYSTEM TO FAIL. As used herein, “High Risk Systems” means any device or system that requires extra
safety functionalities such as fail-safe or fault-tolerant performance features to maintain a safe state
where it is reasonably foreseeable that failure of the device or system could lead directly to death,
personal injury, or catastrophic property damage. A device or system with a fail-safe feature in the event
of failure may revert to a safe condition rather than break down, may include a secondary system that
comes into operation to prevent a malfunction, or may operate as a backup in the event of a
malfunction. A device or system with a fault-tolerant feature in the event of failure may continue its
intended operation, possibly at a reduced level, rather than failing completely. Without limitation, High
Risk Systems may be required in critical infrastructure; industrial plants; manufacturing facilities; direct
life support devices; aircraft, trains boats or vehicle navigation or communication systems; air traffic
control; weapons systems; nuclear facilities; power plants; medical systems and facilities; and
transportation facilities.

Third Parties. THE SOFTWARE AND CLOUD SERVICES MAY CONTAIN
INDEPENDENT THIRD PARTY PRODUCTS AND RELY UPON THEM TO PERFORM
CERTAIN FUNCTIONALITY, INCLUDING MALWARE DEFINITIONS OR URL FILTERS AND ALGORITHMS.
MCAFEE MAKES NO WARRANTY AS TO THE ACCURACY OF ANY SUCH THIRD PARTY INFORMATION.

Internet Delays. CLOUD SERVICES MAY BE SUBJECT TO LIMITATIONS, DELAY AND
OTHER PROBLEMS INHERENT IN THE USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS.
MCAFEE IS NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES OR DAMAGES RESULTING FROM
SUCH PROBLEMS.

Security. No data transmission over the Internet can be guaranteed to be secure. McAfee is not
responsible for any interception or interruption of any communications through the Internet or
networks or systems outside McAfee’s control. Customer is responsible for maintaining the security of
its networks, servers, applications and access codes.

PARTNER ACCESS. Customer acknowledges and agrees that if the Cloud Services are purchased through
a Channel Partner, the Channel Partner may have access to: (1) Customer Data; and (2) system
administration of Customer’s account, including the ability to configure the account and applicable
policies.
LIMITATIONS OF LIABILITY.

a. NO CONSEQUENTIAL DAMAGES. UNDER NO CIRCUMSTANCES WILL MCAFEE OR ITS LICENSORS BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, EXEMPLARY, CONSEQUENTIAL, OR EXTRA-CONTRACTUAL DAMAGES OF ANY KIND OR LOSS OF PROFITS, LOSS OF GOODWILL, LOSS OF PERSONNEL SALARIES, COMPUTER OR SYSTEM FAILURE OR MALFUNCTION, COSTS OF OBTAINING SUBSTITUTE SOFTWARE OR CLOUD SERVICES, WORK STOPPAGE, DENIAL OF ACCESS OR DOWNTIME, SYSTEM OR SERVICE DISRUPTION OR INTERRUPTION, OR ANY LOST, DAMAGED, OR STOLEN DATA, INFORMATION, OR SYSTEMS. FURTHER, UNDER NO CIRCUMSTANCES WILL MCAFEE OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES ARISING FROM OR RELATING TO ALLEGATIONS OR CLAIMS THAT THE CLOUD SERVICES OR SOFTWARE WERE NOT FAILSAFE, DID NOT OPERATE INTERRUPTION- OR ERROR-FREE, OR DID NOT PROTECT AGAINST ALL SECURITY BREACHES OR ALL POSSIBLE SECURITY THREATS, MALFUNCTIONS, MALICIOUS CODE OR OTHER VULNERABILITIES OR ERRORS IN ANY CLOUD SERVICES OR SOFTWARE CAUSED BY VIRUS, INFECTION, WORM OR SIMILAR MALICIOUS CODE, IN ALL CASES REGARDLESS OF LEGAL THEORY AND WHETHER OR NOT FORESEEABLE, EVEN IF THE EXCLUSIVE REMEDIES PROVIDED BY THIS AGREEMENT FAIL OF THEIR ESSENTIAL PURPOSE AND EVEN IF EITHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OR PROBABILITY OF SUCH DAMAGES. THIS AGREEMENT SHALL NOT IMPAIR THE U.S. GOVERNMENT’S RIGHT TO RECOVER FOR FRAUD OR CRIMES ARISING OUT OF OR RELATED TO THIS CONTRACT UNDER ANY FEDERAL FRAUD STATUTE, INCLUDING THE FALSE CLAIMS ACT, 31 U.S.C. 3729-3733.

b. DOLLAR CAP. REGARDLESS OF WHETHER A CLAIM FOR DAMAGES IS BASED IN CONTRACT, TORT OR ANY OTHER LEGAL THEORY, IN NO EVENT WILL THE AGGREGATE TOTAL LIABILITY OF MCAFEE OR ITS LICENSORS UNDER THIS AGREEMENT OR IN CONNECTION WITH THE SUBJECT MATTER OF THIS AGREEMENT EXCEED (a) FOR MONTHLY CUSTOMERS, TO THE FEES PAID UNDER THIS AGREEMENT FOR THE TWO (2) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM OR (b) FOR ANNUAL CUSTOMERS, TO THE FEES PAID UNDER THIS AGREEMENT FOR THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH CLAIM, LESS THE
AGGREGATE OF ALL AMOUNTS PAID BY SUCH LIABLE PARTY UNDER THIS AGREEMENT OR IN CONNECTION WITH ITS SUBJECT MATTER ON ACCOUNT OF PREVIOUS EVENTS OF LIABILITY. THESE LIMITATIONS DO NOT APPLY TO MCAFEE’S INDEMNIFICATION OBLIGATIONS; TO MCAFEE’S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT; OR TO ANY LIMITATION TO THE EXTENT PROHIBITED BY APPLICABLE LAW.

RISK ALLOCATION. The exclusions and limitations of liability specifically provided by this Agreement allocate between the parties the risks under this Agreement, some of which may be unknown or undeterminable. The exclusions and limitations were a material inducement for the parties to enter into this Agreement, and the parties have relied upon them in determining whether to enter into this Agreement. Each party expressly agrees to these exclusions and limitations and acknowledges that without them, the fees charged for the Cloud Services or Software would be higher or would not be offered under this Agreement.

ACTIONS. Except for claims related to non-payment, or to Customer’s breaches of Section 2 (Right of Use and Restrictions), Section 8 (Confidentiality) or Section 21 (Compliance), neither party may bring any legal action for any relief arising out of any matter relating to this Agreement more than 6 years after the party knew or should have known of the event giving rise to the claim or action.

[RESERVED]

MCAFEE INDEMNITY.

McAfee will indemnify and, at its election, defend Customer against claims asserted against Customer in any suit or proceeding for direct patent or copyright infringement, or for McAfee’s trade secret misappropriation, asserted against the Cloud Services or Software, as and in the form provided by McAfee under this Agreement alone and not in combination with anything.

Notwithstanding anything else, McAfee has no obligation under this Section 15 (McAfee Indemnity) with respect to the following: (a) any claim (such as a counterclaim) that is made in response to a suit or proceeding first filed by Customer, including, without limitation, alleging patent infringement; or (b) any claim to the extent actually or allegedly based on any of the following: (i) elements or features in, or operation of, software, services, or other material not supplied by McAfee, (ii) McAfee’s inclusion or use of software, services, technology, or material provided by Customer, (iii) McAfee’s compliance with Customer’s designs, specifications, or instructions, (iv) modification of any Software by anyone other than McAfee, (v) use of any Cloud Services or Software where that use is contrary to the specifications or instructions for use, or the terms of this Agreement, (vi) combination of any Cloud Services or Software with anything, (vii) the Cloud Services or Software implements or complies with, in whole or in part, as provided or when used, a Standard, (viii) Customer willfully infringed, (ix) McAfee, Customer, or the Cloud Services or Software indirectly infringes, including by inducing or contributing to another’s infringement, or (x) activity that occurs after Customer is notified of the claim and is provided with modifications or other action that would avoid the claimed infringement.
McAfee’s indemnity obligations are conditioned on Customer’s prompt written notice to McAfee of a claim and on Customer’s tender to McAfee of the right to control and conduct the defense and any settlement of the claim, to the extent permitted under 28 U.S.C. § 516. Customer must fully and timely cooperate with McAfee and provide McAfee with all reasonably requested authority, information, and assistance. McAfee is not responsible for any costs, expenses, or compromise incurred or made by Customer without McAfee’s prior written consent.

At its option, McAfee will control and conduct the defense and any settlement of indemnified claims. McAfee, in its sole discretion and at its own expense, may (a) procure for Customer the right to continue using the Cloud Services or Software; (b) replace any affected Cloud Services or Software with non-infringing Cloud Services or Software; (c) modify any affected Cloud Services or Software so that it becomes non-infringing; or (d) upon McAfee’s receipt of Customer’s written representation and promise that it has removed all instances of the affected Software and will not use the affected Software and Cloud Services, credit or refund to Customer a pro-rata portion of the amounts already paid by Customer for the affected Cloud Services for the remainder of the applicable License Period.

The indemnity provided in this Section 15 (McAfee Indemnity) states McAfee’s entire obligation and liability and Customer’s exclusive remedy for claims of patent or copyright infringement, or trade secret misappropriation, by the Cloud Services or Software. This indemnity is personal to Customer and may not be assigned, transferred, or passed through to any third party.

Nothing contained herein shall be construed in derogation of the U.S. Department of Justice’s right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

WAIVER. A party’s failure or delay in enforcing any provision of this Agreement will not operate as a waiver of the right to enforce that provision or any other provision of this Agreement at any time. No waiver of any provision of this Agreement will be valid unless in writing, specifying the provision to be waived, and signed by the party agreeing to the waiver.

GOVERNING LAW; DISPUTE RESOLUTION. This Agreement and any dispute arising out of or relating to it will be governed by the Federal laws of the United States, without regard to conflict of laws principles. The parties exclude the application of the United Nations Convention on Contracts for the International Sale of Goods (1980).

NOTICES. All legal notices to McAfee under this Agreement must be addressed to “Attention: Legal Department” 5000 Headquarters Dr., Plano, TX 75024. All legal notices to Customer may be sent using the contact information on file with McAfee, as specified in the registration information provided by Customer when purchasing or registering for the Cloud Services. Notices shall be deemed effective upon receipt. It is Customer’s obligation to ensure McAfee has the most current contact information.

[RESERVED]

ASSIGNMENT. Neither party may assign this Agreement, whether by contract, operation of law or otherwise, without the prior written permission of the other party. Any attempt by Customer to assign this Agreement, including any rights, duties, or obligations under this Agreement, without the other party’s written consent will be a material breach of this Agreement and will be null and void.
COMPLIANCE. Each Party will comply with all applicable laws in the conduct of its business with respect to its rights and obligations under this Agreement, including, without limitation, applicable privacy and export control laws and regulations, the U.S. Foreign Corrupt Practices Act, and other applicable anti-corruption laws. Customer may not, directly or indirectly, export or transmit any Licensed Products or technical data (or any part thereof) or any process or service that is produced by any Licensed Products, to any country to which such export or transmission is restricted by applicable law, without the authorization, if required, of the Bureau of Industry and Security of the U.S. Department of Commerce or any such other applicable governmental entity as may have jurisdiction over such export or transmission. Customer will not use the Licensed Products for the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, demilitarization, destruction, processing, use, configuration, adaption or modification of any defense, military, intelligence, nuclear, or space article or activity, or missile technology including, without limitation, those items enumerated on (a) Wassenaar Arrangement’s Sensitive List, Very Sensitive List and/or Munitions List; (b) the International Traffic in Arms Regulations (“ITAR”) United States Munitions List (“USML,” 22 C.F.R. pt. 121); or (c) the Common Military List of the European Union, unless authorized by the U.S. Government by regulation or specific license. Customer will not discuss, disclose, or release to McAfee any Confidential Information directly related to any defense, military, intelligence, nuclear, or space article or activity. Customer will not transfer, resell, divert, export or re-export any Licensed Products or any related technical information or materials (i) into any U.S. embargoed countries, or (ii) to any person or entity listed on a denial order published by the U.S. government or any other applicable government. Customer represents and warrants that neither the Bureau of Industry and Security nor any other agency or government has suspended, revoked or denied Customer’s export privileges and that Customer will not provide any Licensed Products to any person or entity whose export privileges have been suspended, revoked, or denied. McAfee products may require authorization from the U.S. and other applicable authorities including, without limitation, the European Union, prior to export, import or use restrictions in other countries. Additional information regarding compliance with export control laws can be found at: http://www.mcafee.com/us/about/export-compliance.aspx.

NOTICE TO U.S. GOVERNMENT END USERS: The Software and Cloud Services are deemed to be "commercial computer software" and "commercial computer software documentation," pursuant to DFAR Section 227.7202 and FAR Section 12.212, if either is applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software or Cloud Services by the United States Government shall be governed solely by the terms of this Agreement and is prohibited except to the extent expressly permitted by this Agreement.

FORCE MAJEURE. Excusable delays shall be governed by FAR 52.212-4(f).

ENTIRE AGREEMENT. This Agreement represents the entire agreement between McAfee and the Ordering Activity with regard to Cloud Services and expressly supersedes and cancels any other communication, representation or advertising whether oral or written, on the subjects herein. This Agreement may not be modified except by a written addendum issued by a duly authorized
representative of McAfee and duly warranted Contracting Officer. However, this Agreement, including without limitation its termination, has no effect on any signed nondisclosure agreements between the parties, which remain in full force and effect as separate agreements according to their terms. The express provisions of this Agreement control over any course of performance, course of dealing, or usage of the trade inconsistent with any of the provisions of this Agreement. The provisions of this Agreement will prevail absent any agreed-upon different, conflicting, or additional provisions that may appear on any purchase order, acknowledgment, invoice, or other writing issued by Customer in connection with this Agreement.

SEVERABILITY. The Parties intend that if a court holds that any provision or part of this Agreement is invalid or unenforceable under applicable law, the court will modify the provision or part to the minimum extent necessary to make it valid and enforceable, or if it cannot be made valid and enforceable, the court will sever and delete the provision or part from this Agreement. Any change to or deletion of a provision or part of this Agreement under this Section will not affect the validity or enforceability of the remainder of this Agreement, which will continue in full force and effect.

REMEDIES. All remedies available to either party for breach of this Agreement are cumulative and may be exercised concurrently or separately, and the exercise of any one remedy will not be deemed an election of such remedy to the exclusion of other remedies.

RELATIONSHIP. The relationship of McAfee and Customer established by this Agreement is that of independent contractors, and nothing contained in this Agreement (a) gives either party the power to direct and control the day-to-day activities of the other party; (b) constitutes the parties as partners, joint ventures, co-owners or otherwise as participants in a joint or common undertaking; or (c) allows either party to create or assume any obligation on behalf of the other party. The relationship contemplated by this Agreement is non-exclusive and does not prohibit either party from entering into any arrangements with any third parties. Each party understands and acknowledges that (a) the other party may develop or acquire technology, software, hardware, and data for its own products and services, and that existing or planned products and services developed or acquired by a party, may contain ideas or concepts similar or identical to those in the Confidential Information or Licensed Products under this Agreement; and (b) entering into this Agreement does not preclude a party from developing or acquiring any products without obligation to the other party.

SUPPLEMENTAL TERMS; GRANT LETTER. In the event of a conflict between a Grant Letter, the Supplemental Terms and/or the Subscription Agreement, the Supplemental Terms shall control over the Grant Letter and Subscription Agreement, but solely as to the relevant Service, and the Subscription Agreement shall control over the Grant Letter.

THIRD PARTIES. All warranty disclaimers and limitations of remedies and damages in this Agreement that are applicable to McAfee (including, without limitation, the warranty disclaimers and limitations of liability) also extend to and apply in respect of McAfee’s affiliates, third party supplies and licensors who are GSA Schedule 70 contract holders. Except as provided in this Section (Third Parties), the parties do not intend, nor may any clause of this Agreement be interpreted, to create under this Agreement any obligations or benefits to, or rights in, any third party from either McAfee or Customer.
SUPPLEMENTAL TERMS AND CONDITIONS

A. On-Premise Software License

The following terms and conditions ("Supplemental Terms") apply to all Customers using OnPremise Software, and are incorporated into the Agreement:

DEFINITIONS. Defined terms used in these Supplemental Terms shall have the meanings set forth in the Subscription Agreement or the meanings given below.

a. “On-Premise Software” means Software that is identified in the applicable Grant Letter and that can be used without any Cloud Services. On-Premise Software may also include additional features or functionality that can be accessed only with either a current subscription or active support contract to certain Cloud Services, as required by the specific offering.

ON-PREMISE SOFTWARE LICENSE AGREEMENT. All On-Premise Software is delivered subject to the McAfee End User License Agreement ("EULA"), which is attached hereto. The terms of this Subscription Agreement and the Supplemental Terms and Conditions are intended to supplement the EULA with respect to On-Premise Software.

CLOUD SERVICES REQUIREMENT. Certain features or functionality of the On-Premise Software require either a current subscription or an active support contract to access accompanying Cloud Services. Customer’s purchase of a license for On-Premise Software includes only the features and functionality of the On-Premise Software that do not require Cloud Services, and does not entitle Customer to the accompanying features and functionality of the Cloud Services.

UPDATES AND UPGRADES. After Customer’s purchased support period for On-Premise Software expires, Customer has no further rights to receive any Updates or Upgrades to the On-Premise Software.

B. Free Services

The following terms and conditions ("Supplemental Terms") apply to all Customers using Free Services, and are incorporated into the Agreement:

DEFINITIONS: Defined terms used in these Supplemental Terms shall have the meanings set forth in the Subscription Agreement or the meanings given below.

a. In addition to the definition set forth in the Subscription Agreement, “Cloud Services” includes free versions of the cloud services that McAfee provides to Customer as specified in one or more Grant Letters, including (i) any features or functionality included in a paid subscription for which McAfee no longer charges or which McAfee offers to Customer at no charge in McAfee’s sole discretion, and (ii) other features or functionality that McAfee makes available to Customer without charge, that is labeled as “Pre-Release,” “Limited Release,” “Beta” or otherwise
identified by McAfee as experimental, untested, or not fully functional, and which is not a time-limited trial for Customer’s evaluation purposes (each “Free Services”). “Free Services” also includes any accompanying Software or service that McAfee provides without charge to Customer as a courtesy and in McAfee’s sole discretion.

LICENSE PERIOD. For Free Services, subject to the terms of the Agreement, the License Period continues for as long as McAfee makes such Free Services available to Customer.

McAfee may choose to provide Free Services to Customer prior to, during, or after Customer’s paid subscription to Cloud Services or Software, and any use is subject to the terms of the Agreement then in effect for as long as the Free Services are made available to Customer.

UPDATES / ASSISTANCE / END-OF-LIFE. Any updates or end-user assistance provided for Free Services are provided at McAfee’s sole discretion and may be discontinued at any time. From time to time, at McAfee’s sole discretion, McAfee may elect to discontinue certain Free Services or particular features of the Free Services (“Free Services Termination”). Free Services are specifically excluded from McAfee’s End-of-Life-Policy. Instead, McAfee will make commercially reasonable efforts to provide thirty (30) days’ prior notice to Customer of a Free Services Termination. McAfee has no obligation to provide any Support to Customers for the Free Services.

COMMUNITY FORUM. At their convenience, Customers may exchange ideas and technical insight regarding the Free Services on the Cloud Visibility - Community Edition page located at: https://community.mcafee.com/community/business/data/cloud-visibility.

McAfee does not endorse, warrant or guarantee any information posted on this site and any use of the information is taken at Customer’s sole risk.

DISCLAIMER. Customer acknowledges that the Free Services may contain errors, defects or other problems that could cause system or other failures, security breaches, interruptions and data loss. CONSEQUENTLY, THE LIMITED WARRANTY IN SECTION 11(a) OF THE SUBSCRIPTION AGREEMENT DOES NOT APPLY TO FREE SERVICES. INSTEAD, FREE SERVICES ARE PROVIDED TO CUSTOMER SOLELY ON AN “AS IS” BASIS, AND MCAFEE DISCLAIMS ALL WARRANTIES AND LIABILITY IN CONNECTION WITH THE FREE SERVICES. CUSTOMER ASSUMES ALL RISK OF USE OF FREE SERVICES. In addition, Customer acknowledges that McAfee has not promised or guaranteed to Customer that Free Services will be announced or made available to anyone in the future, that McAfee has no express or implied obligation to Customer to announce or introduce Free Services, and that McAfee is not obligated to introduce a product similar to or compatible with Free Services or any updates to any Free Services.

NO SERVICE LEVEL AGREEMENT. Any Service Level Agreement that, in McAfee’s sole discretion, is offered or may be offered for the Cloud Services, does not apply to Free Services. In the event of a covered outage or other issues with the Free Services, Customer and other users of the Free Services may not make a claim under the Service Level Agreement.

LIMITATION OF LIABILITY. WHERE LEGAL LIABILITY CANNOT BE EXCLUDED, BUT MAY BE LIMITED, THE AGGREGATE LIABILITY OF MCAFEE AND LICENSORS IN CONNECTION WITH THE FREE SERVICES SHALL BE
LIMITED TO THE SUM OF ONE HUNDRED UNITED STATES DOLLARS ($100) (OR THE THEN-CURRENT
VALUE IN THE RELEVANT LOCAL CURRENCY) IN TOTAL.

FREE SERVICE DATA STORAGE. McAfee has no obligation to retain any Customer Data or other Customer
information submitted or collected through the Free Services. McAfee may delete any such Customer
Data and other Customer information at its own discretion and without prior notice to Customer.

Cookie Notice

Our Sites (as defined below) use Cookies and Similar Technologies to ensure that we give our visitors the
best possible experience by providing you personalized information, remembering your marketing and
product preferences, and helping you obtain the right information. You can find out more about Cookies
and Similar Technologies, how we use them, and how to control them below.

Use of Cookies and Similar Technologies

This Notice describes how McAfee (including certain McAfee Affiliates and Service Providers)
(collectively “we” or “us”) uses Cookies and Similar Technologies (such as pixel tags, web beacons, clear
GIFs, JavaScript, and local storage). We will refer to these Cookies and Similar Technologies simply as
“Tracking Technologies” for the rest of Notice. We will also describe what options you may have
regarding Tracking Technologies. This Notice covers the use of Cookies that may be used in connection
with McAfee’s websites, mobile websites, and apps (the “Sites”).

In some cases, we may use Tracking Technologies to collect information that is personally identifiable, or
that can become personally identifiable if we combine it with other information. In such cases, our
Privacy Policy will apply in addition to this Cookie Notice.

What Are Tracking Technologies?

Cookies are small files—usually consisting of letters and numbers—placed on your computer, tablet,
phone, or similar device, when you use that device to visit a website. Cookies are widely used by website
owners and their service providers or partners to make their websites operate, work more efficiently,
and provide analytic information.

These are the different types of Cookies used on our Sites:

Essential Cookies. These Cookies are required for the operation of our Sites (for example, to enable you
to log into secure areas of our website or use a shopping cart). These Cookies enable you to move
around the Sites and use their features. Disabling these Cookies will encumber the Sites’ performance
and may make the features and service unavailable.

Analytics and Customization Cookies. These Cookies allow us to analyze activities on our Sites and on
other sites where we post content in order to improve and optimize the way our Sites work. For
example, we may use these types of Cookies to ensure that visitors can easily find the information they
are looking for. One way we do this is to recognize and count the number of visitors and see how they
move around a Site when they are using it. Analytics cookies also help us measure the performance of
our advertising campaigns in order to help us improve our advertising campaigns and to optimize our
Sites’ content for those who engage with our advertising.
Functionality Cookies. These Cookies are used to recognize you when you return to our Sites. This enables us to personalize our content for you, greet you by name, and remember your preferences (for example, your choice of language or region).

Advertising Cookies. These Cookies record your online activities, including your visits to our Sites, the pages you have visited, and the links and advertisements you have clicked. One purpose of this is to help make the content displayed on our Sites more relevant to you. Another purpose is to allow delivery of advertisements or other communications to you that are designed to be more relevant to your apparent interests. Delivery of interest-based advertising may involve us, our service providers and partners such as publishers, data management platforms, and demand side platforms. For example, if you look at a page on one of our Sites, we may cause an advertisement to be delivered to you, on our Site or on other sites, for products referenced on that page or for similar products and services. We and our service providers and partners may also append other data to information collected by these Cookies, including information obtained from third parties, and share this information with third parties for the purpose of delivering ads to you.

Flash Cookies. A Flash Cookie is a small data file placed on a computer using Adobe Flash or similar technology that may be built into your computer or downloaded or installed by you to your computer. We use these technologies to personalize and enhance your online experience, facilitate processes, and personalize and store your settings. Flash cookies may help our website visitors to, for example, set volume preference associated with a video experience, play games, and perform surveys. They help us improve our sites by measuring which areas are of greatest interest to guests. They may be recognized by other sites or by our marketing or business partners. Flash cookies are different from browser cookies and the cookie management tools provided by your browser may not remove Flash cookies. Click here to learn how to manage privacy and storage settings for Flash cookies. If you disable Flash cookies or other similar technologies, please be aware that you may not have access to certain features and services that make your online experience more efficient and enjoyable.

Web Beacon. A Web Beacon is a very small clear picture file used to keep track of your navigation through a single website or a series of websites. They may also be referred to as “Web Bugs” or “Clear Gifs.” Web Beacons may be used with cookies to gain an understanding of how a website’s users navigate through the website.

How Do We Collect and Use Other Information?

We and our service providers may use Tracking Technologies for a variety of purposes, including to:

- Help us and third parties obtain information about your visits to the Sites;
- Process your orders;
- Analyze your visiting patterns to improve our Sites;
- Deliver advertising, communications, and content from us and third parties, on our Sites and those of third parties, specific to your interests;
- Remember your language and other preferences;
- Help you obtain information you are looking for;
Provide a safe and secure service for online transactions; Measure how many people use our Sites, and how they use them;

To keep our Sites running efficiently.

If you register on one of our Sites, or otherwise provide us with your personal information, we may associate that information with other information we collect from or about you, information regarding your use of our Sites, or information we receive about you from third parties. We may use this combined data for purposes consistent with our Privacy Policy, including for marketing.

How Long Do Tracking Technologies Stay on My Device?

Some Cookies will stay on your device between browsing sessions—they do not expire when you close your browser. These Cookies are called “persistent” Cookies. The length of time a persistent Cookie stays on your device varies from Cookie to Cookie. We and others use persistent Cookies for a variety of purposes, such as to store your preferences so that they are available for the next visit, and to keep a more accurate account of how often you visit our Sites, how often you return, how your use of the Sites may vary over time, and the effectiveness of advertising efforts.

Other Cookies operate from the time you visit our Site to the end of that particular web browsing session. These Cookies expire and are automatically deleted when you close your Internet browser. These Cookies are called “session” Cookies.

Who Puts Tracking Technologies on My Device?

Cookies may be placed on your device by McAfee as the Site operator. These Cookies are called “first party” Cookies. Some Cookies may be placed on your device by a party other than McAfee. These Cookies are called “third-party” Cookies. For example, a McAfee partner may place a thirdparty Cookie to enable online chat services.

Cookies may also be used that allow us and third parties to know when you visit our Sites, and to understand how you interact with emails, advertisements, or other content. Through Cookies, aggregate and other information not identifying individual users (such as your operating system, browser version, and the URL you came from, including from emails and advertisements) may be obtained and used to enhance your experience and understand traffic patterns. This technology counts the number of users who visit a particular service from specific banner advertisements outside the McAfee Site or who clicked on links or graphics included in email newsletters received from McAfee. It is also used as a tool to compile aggregated statistics about how McAfee Sites are used, to perform analytics and help us to optimize our Sites, and to help serve you advertising based on your interests, as described in further detail below.

How Does McAfee Use Online and Mobile Advertising?

We and third parties, including technology partners, and service providers engage in interest-based advertising to deliver advertisements and personalized content that we and other advertisers believe will be of interest to you. To the extent third-party vendors are using Cookies to perform these services for us, McAfee does not control the use of this technology or the resulting information, and is not responsible for any actions or policies of such third parties. We identify some resources in this Notice (see “How do I Manage Tracking Technologies” below) that can help you.
Ads may be delivered to you based on your online or mobile behavior (on McAfee Sites or other sites), your search activity, your responses to one of our advertisements or emails, the pages you visit, your general geographic location, or other information. These ads may appear on our Sites or on third-party websites. The technology partners with whom we work to help us conduct interest-based advertising may be members of self-regulatory associations such as the Network Advertising Initiative (NAI) and the Digital Advertising Alliance (DAA). For Sites directed at persons located in the European Union, we may work with technology partners who are members of the European Digital Advertising Alliance (eDAA). You may also see advertisements for third parties on our Sites or other websites or properties, based on your visits to, and activities on, our Sites and other sites.

How Do I Manage Tracking Technologies?

You can decide whether or not to accept Cookies. One way you can do this is through your Internet browser’s settings. Most Internet browsers allow some control of most Cookies through the browser settings (Please note that if you use your browser settings to block all Cookies you may not be able to fully use the Site.). You can find information online about how to manage Cookies. For example, the following links provide information on how to adjust the Cookies settings on some popular browsers:

Apple Safari
Google Chrome
Microsoft Internet Explorer
Mozilla Firefox

You can also use a browser plug-in such as Ghostery or the Tracking Protection List from TRUSTe. (A browser plug-in is a piece of software which adds extra capabilities to your browser—for example, to play video or scan for viruses). Adobe Flash Player is software for viewing multimedia on a computer. Websites that use Adobe Flash may store Flash Cookies. Flash Cookies may also be known as Flash Local Shared Objects (LSOs). McAfee may use Flash LSOs to provide special content, such as video and animation playback.

To find out more about interest-based advertising and your choices, visit these sites: Digital Advertising Alliance, the Network Advertising Initiative, and the InteractiveAdvertising Bureau (IAB) Europe. You can opt out of the use of Cookies to tailor content or advertising to you by visiting the following links. Note that if you choose to opt out, you won’t necessarily see fewer ads. However, the ads you see may be less relevant to your interests.

http://www.networkadvertising.org/managing/opt_out.asp
http://www.aboutads.info/choices

How Does McAfee respond to a Do Not Track Signal?

There is currently no industry agreed upon response to a Do Not Track signal. At this time, McAfee Services and Sites do not respond to a user’s Do Not Track signal.

Privacy
We are committed to good privacy practices. For more information about our approach to privacy see our Privacy Notice and the Code of Conduct.

How to Contact Us

If you have any questions about how we use Cookies, you can contact us using the information set forth below. Please include your contact information and a detailed description of Cookie concern.

McAfee LLC
Attn: Legal Department – Privacy Office,
5000 Headquarters Drive, Plano TX 75024
Email: privacy@mcafee.com
Telephone: +1 972-963-7902

This Notice updates and supersedes previous versions. We may change this Notice at any time. Changes to this Notice must be agreed to by both parties in writing prior to becoming effective. The “LAST UPDATED” section at the bottom of this page lists when this Notice was last revised. LAST UPDATED: April 3, 2017

McAfee Privacy Notice
Effective Date: April 3, 2017

This Notice provides information about data we collect, use, and share, and our commitment to using the personal data we collect in a respectful fashion.

Privacy Notice Overview

Why Do We Collect Information and Data?

What Kinds of Personal Information Do We Collect?

How Do We Collect Information?

How Do We Use Personal Information?

When Do We Share Personal Information?

Third-Party Advertising

What Security Measures Do We Have?

What Choices Do You Have About Your Personal Information?
We at McAfee, LLC and our affiliates with whom you have a business relationship ("McAfee", "we", "us") care deeply about privacy, security, and online safety, all of which are a significant part of our essential mission: to protect users of our products and services ("you", "your") from the risks of theft, disruption, and unauthorized access to their online information and activities. This Privacy Notice ("Notice") is designed to inform you about how we collect, use, and share your personal information.

This Privacy Notice applies to personal information we obtain from individuals through our websites, products, services, and web-based applications (collectively, the "Services"). In addition, some of our products and services, such as our wide array of mobile applications ("Apps"), are subject to a separate privacy notice. If a separate privacy notice applies to a particular product or service, for example, such as our Mobile App Privacy Statement, we will post it on our website (our "Site").

When you access or use our Services, you acknowledge that you have read this Notice and understand its contents. Your use of our Services and any dispute over privacy is subject to this Notice and our Terms of Service (including any applicable limitations on damages and the resolution of disputes).

As McAfee grows, our business changes, and we may update this Notice, or other privacy notices that we establish for individual products, at any time as we deem appropriate to reflect those changes. Both parties must agree to the changes in writing prior to the changes going into effective.

Why Do We Collect Information and Data?

We rely on a wide variety of information to run our business. In some instances, this information may include data that could be used to identify a particular individual, otherwise referred to as Personal Information. In this Notice, we will provide multiple examples of how Personal Information we collect may be used and why it is important. For example, when a consumer purchases one of our products we must collect their name, email address, and payment information to complete the transaction. Some of the reasons that we collect Personal Information include to:

Provide our products and services, including our Apps and this Site, and improve them over time;

Allow you to download and purchase products and services;

Personalize and manage our relationship with you, including introducing you to products or services that may be of interest to you or to provide customer support;

Investigate, respond to, and manage inquiries or events;

Work with and respond to law enforcement and regulators; and

Research matters relating to our business such as security threats and vulnerabilities.
What Kinds of Personal Information Do We Collect?

The following are examples of the type of Personal Information that may be collected. The specific kind of information collected will depend on the Services used:

- Contact information (such as name, email address, mailing address, and phone number);
- Payment information (including payment card numbers, billing address, and bank account information);
- McAfee purchase or product/service use history;
- Account log-in credentials;
- Your location;
- Your interests;
- Demographic information;
- Photographs, images, video, and related hash values; or
- Biometric data such as fingerprints or voice recordings.

In addition to the above, we may also collect other information related to user interactions with or use of our Services ("Usage Data"). Much of this Usage Data, for example, clickstream data and aggregate usage statistics, is generally not personally identifying. On the other hand, some of this Usage Data either alone or when combined or linked with your Personal Information, may allow your identity to be discovered. In such cases, we treat the combined data as Personal Information. In many cases, Usage Data is gathered automatically by systems or technology such as cookies (see more information about Information Collected Automatically below).

The following are examples of the type of Usage Data that may be collected by McAfee from your web browser or related to your interactions with our products and services:

- Details about your computers, devices, applications, and networks (including IP address, browser characteristics, device ID, operating system, and language preferences);
- Activities on our websites and usage patterns of products and services (including referring URLs, dates and times of website visits, and clickstream data);
- Details about Internet, App, or network usage (including URLs or domain names of websites you visit, information about applications that attempt to access your network, or traffic data);
- Data about files and communications, such as potential malware or spam (which may include computer files, emails and attachments, email addresses, metadata, and traffic data, or portions or hashes—a hash file is a file that has been converted into a numerical string by a mathematical algorithm—of any of this information).

How Do We Collect Information?

We collect information directly from you, as well as automatically through your use of our Services and, in some cases, from third parties.
Information That You Give Us: Typically the information we collect directly from you are your contact details, payment or billing data, and relationship information like the content of customer service requests that you initiate, reviews you submit on our products, or responses to surveys. You decide how much information to share with us in most cases, but not sharing required information may limit your ability to engage in certain activities, such as payment information required to complete a purchase.

Information Collected Automatically: When you use or interact with our Site and Services, we receive and store information generated by your activity, like Usage Data, and other information automatically collected from your browser or mobile device. This information may include your IP address; browser type and version; preferred language; geographic location using IP address or the GPS, wireless, or Bluetooth technology on your device; operating system and computer platform; purchase history; the full Uniform Resource Locator (URL) clickstream to, through, and from our Site, including date and time; products you viewed or searched for; and areas of our Site that you visited. We also may log the length of time of your visit and the number of times you visit and purchase or use the Services. We may assign you one or more unique identifiers to help keep track of your future visits.

In most cases, this information is generated by various tracking technologies. Tracking technologies may include “cookies,” “flash LSOs,” “web beacons” or “web bugs,” and “clear GIFs”. You can read about how we use cookies and other tracking technologies here and also learn about the choices you can make to limit their use.

Please see our Cookie Notice for more information about the cookies and other similar technologies that we use.

Information from Other Sources: If we receive any information about you from other sources, we may add it to the information we already have about you. For example, if we receive a list of subscribers to a publication and we note that you are a user of our products and also a subscriber, we may combine that information. Examples of information we may receive from other sources includes updated delivery or payment information which we use to correct our records, purchase or redemption information, customer support or enrollment information, page view, search term and search result information from business partners, and credit or identity information which we use to help prevent and detect fraud.

How Do We Use Personal Information?

Every time you turn on a device, connect to a network, or open a file, you are exposed to significant risk from hackers, malware, spyware, and other forms of unauthorized access to your data and systems. Security products and services, such as McAfee’s, are designed to help protect you from these risks.

Security and Threat Detection. By collecting and processing data, including Personal Information, McAfee can help to predict threats and better protect you, your devices, and your information. For example, McAfee may use your information to:

- Analyze data sent to/from your device(s) to isolate and identify threats, vulnerabilities, suspicious activity, and attacks;
- Assess the reputation of a device or file to advise you on whether access should be granted;
- Participate in threat intelligence networks and conduct research and analysis, including market and consumer research and trend analysis; and
Adapt products and services to respond to new threats.

Business Uses. In addition, we may use Personal Information for other business purposes, including to:

- Analyze users’ behavior when using McAfee products and services to customize preferences;
- Establish and manage McAfee accounts;
- Collect and process payments and complete transactions;
- Provide customer support, manage subscriptions, and respond to requests, questions, and comments;
- Communicate about, and administer participation in, special events, programs, surveys, contests, sweepstakes, and other offers and promotions;
- Enable posting on our blogs and other communications;
- Customize, measure, and improve our websites, products, services, and advertising;
- Analyze and develop new products, services, and websites;
- Perform accounting, auditing, billing, reconciliation, and collection activities;
- Prevent, detect, identify, investigate, respond, and protect against potential or actual claims, liabilities, prohibited behavior, and criminal activity;
- Comply with and enforce applicable legal requirements, agreements, and policies; and
- Perform other activities consistent with this Notice.

Processing as Part of the Services. We also process certain information as an integral part of our Services. If you install or use one of our products or services, software will operate in the background of your computer system or device environment to perform specific security and privacy tasks including:

- Spam protection;
- Virus protection;
- Intrusion detection, prevention, and protection;
- Threat prevention and prediction;
- Network defense;
- Data encryption;
- Mobile device lockdown; and
- Back-up and recovery activities.

Product Updating and Reporting. Our products and services may also process certain data to provide updates and reports. These update functions may check your system to see whether files relating to the services need to be refreshed or modernized. For example, products and services may transmit report files to McAfee. These files contain information, including the number of checked, suspicious, infected, or unwanted files or emails, the number of infections, the date and hash values of the detected infections, and the number of false negatives/false positives. The purpose of these reports is to analyze
the frequency of particular infections or the prevalence of threats. McAfee also uses the information to adapt the product to conform to user preferences based on actual use.

Supporting Free Products and Services

We continually make a variety of free products available to our customers. In order to keep these products free, we may use information collected through some of our products, such as information about websites you visit, to support interest-based advertising by us or our partners. We do this by sharing information with trusted third parties about your browser and web browsing activity that does not identify you personally. These companies are not permitted to use the information we provide to them to identify you, and are required to use the information we provide only in accordance with our privacy commitments to you. Our products that use data in this way also include built-in features allowing you to opt out of this sharing.

When Do We Share Personal Information?

We respect the importance of privacy. Other than as provided in this privacy policy, we do not sell your Personal Information, nor do we share it with unaffiliated third parties for their own marketing use, unless we have your consent or we are required by law to do so. Generally, we may disclose the information we collect, including Personal Information, in order to facilitate our provision of the Services or communications with customers (e.g., to service providers who perform functions on our behalf), to operate our business, to advertise or promote our Services, to facilitate changes to or transfers of our business, as required by law, or with your consent.

We may share Personal Information in the following ways:

Current and future members of the McAfee family of companies for the purposes described in this Notice, such as to: (i) provide services and content (e.g., registration, sales, and customer support); (ii) help detect and prevent illegal acts and violations of our policies; and (iii) guide our decisions about our products, services, and communications;

Other users where integral to particular Services where you have chosen to share such information, or where you have posted user content (e.g., comments and reviews, social media posts, photos or locations to groups you create);

Authorized service providers who perform services for us (including cloud services, data storage, sales, marketing, investigations, payment processing, customer support, and bill collection). Our contracts with our service providers include commitments that they agree to limit their use of Personal Information and to comply with privacy and security standards at least as stringent as the terms of this Privacy Notice. Remember that if you provide Personal Information directly to a third party, such as through a link on McAfee’s website, the processing is typically based on their standards (which may not be the same as McAfee’s);

If we believe disclosure is necessary and appropriate to prevent physical, financial, or other harm, injury, or loss, including to protect against fraud or credit risk.

To legal, governmental, or judicial authorities, as instructed or required by those authorities or applicable laws, or in relation to a legal activity, such as in response to a subpoena or investigating suspected illicit activity (including identifying those who use our services for illegal activities). We
reserve the right to report to law enforcement agencies activities that we in good faith believe to be illegal.

In connection with, or during negotiations of, an acquisition, merger, asset sale, or other similar business transfer that involves substantially all of our assets or functions where Personal Information is transferred or shared as part of the business assets (provided that such party agrees to use such Personal Information in a manner that is consistent with this Notice).

In order to provide marketing and advertising content about our products, or other products which may interest you, we may share your Usage Data, as well as anonymized information with third-party ad networks, social media partners, and similar providers. A more detailed discussion of our relationship with third-party advertisers is set forth below under the heading "Third-Party Advertising".

With others only after obtaining your consent. If we want to share Personal Information other than as permitted or described above, we will provide you with a choice to opt in to such sharing and you may choose to instruct us not to share the information.

Your California Privacy Rights - Shine the Light Law

McAfee does not share your Personal Information with non-affiliated third parties for their own marketing use without your permission.

Third-Party Advertising

Advertising is a way for McAfee to subsidize many of our free products and services and also provides a way to inform you about products or services that we think may be of interest to you. We have agreements with third-party advertising companies to display or deliver ads to you while you are on our Site or using some of our other products, like Apps. These third-party advertisers may automatically receive Usage Data when this happens. They may also download cookies to your computer, or use other technologies such as JavaScript and "web beacons" (also known as "1x1 gifs" or "clear gifs") to measure the effectiveness of their ads and to personalize advertising content. Doing this allows the advertising network to recognize your computer or device each time they send you an advertisement. In this way, they may compile information about where individuals using your computer or browser saw their advertisements and determine which advertisements are clicked. Third-Party Advertisers may also serve advertisements to you on other websites, based on their tracking of what content you looked at or interacted with on our Websites. Other than as described in this Notice, we do not give third-party advertisers your contact information such as email address, phone number, or address.

See our Cookie Notice to learn more about how McAfee uses tracking technologies like cookies and how you can opt out of such technologies and advertising. This Notice does not cover the use of cookies or other tracking technologies by any of our advertisers.

If you have provided our Apps with access to your location, our mobile advertising partners may use your location to target advertisements to you. You can use the location features on your device to disable this targeting.
Do Not Track Disclosure: Our Site does not respond to Do Not Track signals. You may, however, disable certain tracking as discussed above (e.g., by disabling cookies). For more information about Do Not Track signals, please click here.

What Security Measures Do We Have?

We use administrative, organizational, technical, and physical safeguards to protect the Personal Information we collect and process. Our security controls are designed to maintain an appropriate level of data confidentiality, integrity, and availability. We regularly test our website, data centers, systems, and other assets for security vulnerabilities.

McAfee handles payment card data in a manner consistent with the Payment Card Industry Data Security Standard (PCI-DSS). For example, when you make a payment on our website using your credit card, we use SSL encryption for transmission of the credit card number.

What Choices Do You Have About Your Personal Information?

We offer certain choices about how we communicate with our users and what Personal Information we obtain about them. Many McAfee products allow users to make choices about the Personal Information collected.

You may choose not to receive marketing communications from us by clicking on the unsubscribe link or other instructions in our marketing emails, visiting the My Account section on our website, or contacting us as specified in the “Contact Us” section below.

Many McAfee products contain settings that allow users or administrators to control how the products collect information. Please refer to the relevant product manual or contact us through the appropriate technical support channel for assistance.

To remove your Personal Information from a McAfee website testimonial, please contact customer service.

If you chose to no longer receive marketing information, McAfee may still communicate with you regarding such things as security updates, product functionality, responses to service requests, or other transactional, non-marketing/administrative related purposes.

How you can access and correct inaccuracies

If you subscribe to McAfee products, you can access and correct the Personal Information in your profile by visiting My Account. Alternatively, you may request access or changes to, or removal of, your Personal Information in accordance with applicable laws by contacting us as indicated below. For some requests, an administrative fee may be charged (where permitted by law). We will advise you of any applicable fee prior to performing your request.

Data Retention

The time periods for which we retain your Personal Information depend on the purposes for which we use it. McAfee will keep your Personal Information for as long as you are a registered subscriber or user of our products or for as long as we have another business purpose to do so and, thereafter, for no longer than is required or permitted by law, or McAfee’s Records Retention Policy, reasonably necessary
for internal reporting and reconciliation purposes, or to provide you with feedback or information you might request. The information we collect may be stored and processed in servers in the United States and wherever McAfee and our service providers have facilities around the globe.

Children’s Privacy

Some of McAfee’s Services provide security features that may be used to monitor children’s activity online, physical location, or when they are using a registered device. McAfee does not knowingly collect Personal Information from children under the age of 13 without first obtaining parental consent in accordance with applicable laws like the Children’s Online Privacy Protection Act of the United States and similar laws around the world. For products that may be used with children, there are options for parents or legal guardians to delete their child’s profile at any time and at the parent or guardian’s option. We do not knowingly use Personal Information from children for any purpose except to deliver the products that are designed to offer family-related or child-related protection Services. If you believe we have collected information from your child in error or have questions or concerns about our practices relating to children, please notify us using the Contact Us details below and we will promptly respond.

Data Transfers

McAfee is headquartered in the United States, and we have operations, entities, and service providers in the United States and throughout the world, including in India. As such, we and our service providers may transfer your personal information to, or access it in, jurisdictions that may not provide equivalent levels of data protection as your home jurisdiction. We will take steps to ensure that your personal information receives an adequate level of protection in the jurisdictions in which we process it. If you are located in the European Economic Area or Switzerland, we provide adequate protection for the transfer of Personal Information to countries outside of the EEA or Switzerland through a series of intercompany agreements based on the Standard Contractual Clauses authorized under the EU Data Protection Directive 95/46/EC.

Links to Other Websites

Our Site may contain links to other websites for your convenience and information. These websites may be operated by companies not affiliated with McAfee. Linked websites may have their own privacy policies or notices, which we strongly suggest you review if you visit those websites. We are not responsible for the content, privacy practices, or use of any websites that are not affiliated with McAfee.

Contact Us

If you have questions or concerns regarding this Privacy Notice, or would like to update information we have about you or your preferences, please contact us by email at privacy@mcafee.com or by one of the following additional methods: In the United States by calling us at +1 972-963-7902 or by writing to us at:

Attn: Legal Department – Privacy Office,
5000 Headquarters Drive, Plano TX 75024

In the European Economic Area by calling us at +44 (0) 1753 217 500 or by writing to us at:
Mobile App Privacy Statement

What We Collect

How We Use Your Information

How We Share Your Information

Your Choices

Security

International Transfers

Data Retention

Children and Minors

Notice to California Residents

Updates to This Privacy Notice

Contact Us

Effective Date: April 3, 2017

McAfee, LLC and our affiliates with whom you have a business relationship (“McAfee”, “we”, “us”) respect your privacy. This Mobile App Privacy Statement (“App Privacy Notice”) describes our privacy practices regarding the collection, use, and disclosure of your personal information through our mobile apps (our “app” or “apps”).

1. What We Collect.

Information you provide:
We may require that you register to use the apps. Registration may require personal information like your email address and name and information like a unique user name or password. In some cases, you may be able to sign in using your Google or Facebook account credentials which will then be used only for the purpose of account access and account management.

The functionality of the apps may require some access to personal information in order to use the apps. This may include contact information such as your name, address, phone number, email address, and unique log-in credentials. The apps may also access unique numeric identifiers assigned to your device such as your mobile advertising ID/IDFA, Bluetooth device IDs, and mobile device ID.

Other types of information may also be collected by the apps such as:

IDs of any Bluetooth devices connected to your mobile device

Media such as photos and videos that you store or consent to give us access to

Device details such as OS, device ID, and device type

List of other apps on your device and information about those applications

Your location

Details of your McAfee product subscriptions such as products used, registration data, product key, and the like

Information about websites that you view and visit

Battery levels, on/off device status

Access to some of the above information (such as your location) may be restricted by your mobile device’s operating system, and your consent will be requested before we may access this information. It is your choice whether you wish to provide consent; however, if you do not provide consent, some functionality of the apps may be restricted.

You may also have the opportunity to voluntarily provide additional information from time to time that is not required by the apps but may improve your experience. Information we collect automatically from your device and apps

In addition to the above information, the apps automatically collect other device-related information and app performance data. This includes crash logs to assess application usability and performance, length of time spent on the apps, and other aggregate or statistical information. Location data may be automatically collected, such as by GPS, for the purpose of providing certain features of the apps. This data is transmitted and stored separately from any personal information processed by the apps and contains no information that can reasonably be used to directly identify you.

How We Use Your Information.

In addition to providing and improving the apps and related services, we use your personal information to communicate with you, including to send you notifications and alerts and for in-app advertising and marketing (in accordance with your marketing preferences), to respond to your requests (such as for technical support or customer service), and for research and analytics. In addition to the uses described
in this App Privacy Notice, we may use your personal information as otherwise permitted by applicable law.

Some apps may use information about the websites you visit and the apps installed on your device to show you more relevant ads. When we do this, we will provide you notice of these activities and the opportunity to opt out.

How We Share Your Information.

Third-party service providers and affiliated companies

Other than as described in this App Privacy Notice, we do not sell, rent, or share information that identifies you personally like your name, email address, phone number, or address. We may need to share the information we collect through the apps with third-party service providers in order to support the apps, their features, and their services, including customer services and technical support, and with our affiliated companies.

We may share the advertising identifier assigned to your device along with information about the websites you visit or the apps installed on your device with third-party service providers so that they can use that information to help show you ads that are more likely to be relevant to your interests. This information does not identify you personally.

Some of our providers may use your information in a format that does not directly identify you for their own business purposes (such as to improve their own services). For example, they may track the number of customer support calls required before an issue is resolved in order to improve resolution time. Our contracts do not permit our third-party service providers to use your personal information in ways that are inconsistent with this App Privacy Notice.

Third-party service provider terms

Some of our third-party service providers may have additional terms and choices that apply to your information which we are required to make available to you as follows:

Google Maps: If the app uses Google Maps’ API, it is governed by Google’s Privacy Policy. Certain Maps API(s) store and access cookies and other information on end-users’ devices.

The Facebook Audience Network: We are a member of the Facebook Audience Network. This provides a way for companies to display their ads to Facebook users in apps and websites that are also part of the network. Facebook helps tailor the ads so that they are relevant and useful. You can use Facebook’s ad preferences tool to view, add, and remove your preferences, including whether you receive these tailored ads, including in our apps. We encourage you to review Facebook’s data policy and privacy basics. Ads in our apps may also include an Ad Choices opt-out icon so you can opt out directly from our app.

Other ways your personal information may be shared

Your personal information may also be used and shared with law enforcement, government representatives, or others if required by law, in connection with a sale purchase, merger, or reorganization, or when we believe it is necessary to protect our rights, property, or safety, to comply with a judicial proceeding, court order, or legal process—such as evidence in litigation in which we are
involved. In the case of a sale or purchase we will instruct the entities to which we transfer your personal information only to use it in a manner consistent with this App Privacy Notice.

Your Choices.

You may request access to view, modify, update or remove the personal information that we have related to your use of the apps by contacting us using the details supplied in the "Contact Us" section below. You can unsubscribe from our marketing-related messages at any time by following the unsubscribe instructions included within each marketing-related message sent to you or by using the details in the "Contact Us" section. We will comply with requests within the time frames required by applicable law. Please note that if you choose not to receive marketing-related emails from us, we may still send you important administrative and transactional messages related to the apps and services (“service notifications”).

You may have the option to limit the use of information about your device for purposes of serving ads that are targeted to your interests through your device settings (called “Limit Ad Tracking” on iOS devices and “Opt Out of Interest-Based Advertising” on Android devices).

Security.

We take reasonable technical, administrative, and physical measures to protect the personal information provided, but you must understand that no app or internet transmission can ever be guaranteed 100% secure. Where personal data collected is stored on your device, security is through your device’s own secure storage facilities. You should also take care to protect the secrecy of your account user name and password and to protect the personal information that is stored on your device.

International Transfers.

We are a U.S.-based, global company. As such, we may transfer, store, and process your personal information in the United States (U.S.) or to any of our group companies worldwide when processing that information for the purposes described in this App Privacy Notice. We may also transfer your personal information to our third-party service providers, who may be located in a different country than you.

Personal information collected by us from the European Economic Area and Switzerland is protected in accordance with applicable legal requirements implemented through intra-group agreements incorporating the standard model contractual clauses recognized by the Directive 95/46/EC of the European Parliament and the Council, also known as the Data Protection Directive ("the Directive").

Data Retention.

We retain account information, such as your name, account credentials, and email for the lifetime of your account. However, if you are not an active user of the app (as determined by number of log-in attempts) your account and all data will be deleted after a reasonable period of time. If your data is deleted, you may have to establish a new account to begin using the app again. In some products, data may be stored locally on your device as well as remotely on our (or our service provider’s) systems. Generally, if you delete the apps on your device, any data stored locally on the device will be deleted; however, data on servers elsewhere may remain. You can request that we delete your personally
identifiable information on our app servers by sending a written request to us as instructed in the Contact Us section below. Your request must provide your name, any app-specific user ID, email address, and the name of any apps subject to your request. We will retain these communications for our record keeping purposes.

Use of Services by Minors.

We comply with the Children’s Online Privacy Protection Act of the United States and similar laws around the world where applicable to our products and services. We do not knowingly collect personal information from children without proper parental consent. If you believe that we may have improperly collected personal information from someone under the applicable age of consent in your country, please let us know using the methods described in the Contact Us section and we will take appropriate measures to investigate and address the issue promptly.

Notice to California Residents.

Section 1798.83 of the California Civil Code requires us to tell you that we do not share your personal information with third parties for their direct marketing purposes.

Updates to this App Privacy Notice.

From time to time we may update this App Privacy Notice and/or our Privacy Notice for legal, regulatory, or business reasons. Any such changes will presented for review and will be agreed to by both parties in writing

Contact Us.

If you have questions or concerns about our privacy practices, you can send a letter to the postal address listed below. To help us most effectively respond to your query, please include your contact information, name of the Service or website, and a detailed description of your request or privacy concern.

McAfee LLC
Attn: Legal Department – Privacy Office
5000 Headquarters Drive, Plano TX 75024
Email: privacy@mcafee.com
Telephone: +1 972-963-7902

If you are located in the European Economic Area, please write to:
227 Bath Road
Slough, Berkshire
SL1 5PP United Kingdom
Telephone: +44 (0) 1753 217 500 Email: privacy@mcafee.com