

**AGREEMENT**  
(Government Customers – GSAMultiple Award Schedule Contract)

This agreement (“Agreement”) is entered into effective as of \_\_\_\_\_, 20\_\_, (the “Effective Date”) between Cisco Systems, Inc., on behalf of itself and for the benefit of its affiliates, including, without limitation, Duo Security, Inc., a Delaware corporation with a registered address at 123 N. Ashley Street, Ann Arbor, MI 48104 (“Duo Security”), and the Federal Customer purchasing from the GSA Multiple Award Schedule (MSA) contract (“Customer”). This Agreement, including the Terms and Conditions containing, among other things, warranty disclaimers, liability limitations and use limitations, includes and is effective for the Order Form and any subsequent renewals, purchase orders or Order Forms (submitted in written or electronic form) related to Customer’s subscribing to the Services unless different or additional terms are expressly agreed to in writing and signed by both parties. There will be no force or effect given to any different or additional terms contained in any purchase order or similar form issued by either party, even if signed by the parties unless such terms are included in an amendment in accordance with the terms of Section 14.3 of this Agreement. Each party’s acceptance of this Agreement was and is expressly conditional upon the other’s acceptance of the terms contained in this Agreement to the exclusion of all other terms. Capitalized terms shall have the meanings ascribed to them in the Terms and Conditions.

**TERMS AND CONDITIONS**

**1. DEFINITIONS**

1.1 “Customer” means the U.S. Government customer that has placed an order with for the Services and thereby signed up for the Services and agreed to the terms of this Agreement under the GSA MAS contract. The Department of Veterans Affairs shall not be a Customer and cannot purchase from Duo Security under the GSA MAS contract.

1.2 “Customer Data” means any information or data about Customer or Users (and its and their staff, customers or suppliers, as applicable), that is supplied to Duo Security by or on behalf of Customer or any User in connection with the Services, or which Duo Security is required to access, generate, process, store or transmit pursuant to this Agreement, including (but without limitation) information about Customer’s and Users’ respective devices, computers and use of the Services.

1.3 “Customer Personal Data” means any Customer Data that is personal data (as defined under the DPA).

1.4 “Data Protection Laws” means the DPA, EC Directive 95/46/EEC, EC Directive 2002/58/EC, the UK Privacy and Electronic Communications (EC Directive) Regulations 2003 and any other applicable data protection laws, regulations and legally binding codes of practice from time to time in force applicable to the performance of a party’s obligations under this Agreement.

1.5 “Documentation” means guides, instructions, policies and reference materials provided to Customer by Duo Security in connection with the Services, including the documentation located at <https://www.duosecurity.com/docs>, which may be amended from time to time.

1.6 “DPA” means the UK Data Protection Act of 1998.

1.7 “Duo Mobile Software” means all Duo Security proprietary mobile applications (available on iPhone, Android, Palm, Blackberry, Windows Mobile and other supported mobile devices) used in providing the Services, and any updates, fixes and/or patches developed from time to time.

1.8 “Fees” means the applicable fees as set forth on the Order Form.

1.9 “Hardware Tokens” mean hardware security tokens purchased by Customer under an Order Form.

1.10 “Integration Software” means (a) Duo Security proprietary software and (b) open source software used in providing the Services which integrates with Customer’s network or application, including SSL or other VPN, Unix operating system, Microsoft application, and/or web application, as provided in the Documentation and any updates, fixes and/or patches developed from time to time.

1.11 “Intellectual Property Rights” means all patents, registered designs, unregistered designs, design rights, utility models, semiconductor topography rights, database rights, copyright and other similar statutory rights, trade mark, service mark and any know how relating to algorithms, drawings, tests, reports and procedures, models, manuals, formulae, methods, processes and the like (including applications for any of the preceding rights) or any other intellectual or industrial property rights of whatever nature in each case in any part of the world and whether or not registered or registerable, for the full period and all extensions and renewals where applicable.

1.12 “Order Form(s)” means the order forms through which the Government customer purchases the Duo Security Services from Duo Security under the GSA MAS contract for the initial order for the Service, and any subsequent order forms issued to Duo Security, specifying, among other things, the maximum number of Users, the initial Term, the purchase of any Hardware Tokens, the Fees, telephony credits (if any), and such other charges and terms as agreed between the parties.

1.13 “Performance Data” means data with respect to usage and other aggregate measures of the Services’ performance that Duo Security may collect from time to time.

1.14 “Services” means the products and services that are ordered by and/or made available to Customer under a free trial or an Order Form (including, where applicable, the Software, Hardware Tokens and services using only the Duo Mobile Software) and made available online by Duo Security, including associated offline components, as described in the Documentation.

1.15 “Service Level Agreement” or “SLA” means the description of support provided to Customers and its Users and of the availability of the Services attached to this document as Appendix A.

1.16 “Software” means the Integration Software and Duo Mobile Software.

1.17 “Telephony Credits” mean credits for Customer’s Users to provide authentication by telephone or SMS.

1.18 “Term” means the subscription term indicated on the Order Form and any subsequent renewal terms.

1.19 “User” means any user of the Services who Customer may authorize to enroll to use the Services under the terms of this Agreement.

## **2. SERVICES FOR CUSTOMER; DUO SECURITY OBLIGATIONS**

2.1 Subject to and conditioned on the GSA MAS Contractor’s receipt of payment of the Fees and in any event, subject to full compliance with all other terms and conditions of this Agreement, Duo Security grants Customer and Users a non-exclusive, non-sublicensable, non-transferrable license to access and use the Services, along with such Documentation as Duo Security may make available during the Term.

2.2 The Services and SLA are subject to modification from time to time at Duo Security’s sole discretion, provided the modifications do not materially diminish the functionality of the Services provided by Duo Security and the Services continue to perform according to the description of the Services specified in Section 2.3 in all material aspects. Customer shall have the right to terminate the Agreement pursuant to Section 10.2 without any penalty if (i) a material modification to the Services or the SLA is made which materially diminishes the functionality of the Services or materially diminishes the SLA, (ii) Duo Security has not obtained Customer’s consent for such modifications and (iii) Duo Security does not provide a remedy in the cure period stated in Section 10.2.

2.3 Duo Security will make the Services available and the Services will perform substantially in accordance with the description of the services found at <http://www.duosecurity.com/editions>. Notwithstanding the foregoing, Duo Security reserves the right to suspend Customer’s (or any of its Users’) access to the Services: (i) for scheduled or emergency maintenance, or (ii) as it deems reasonably necessary to respond to any actual or potential security concerns.

2.4 Subject to full compliance with the terms and conditions of this Agreement, Duo Security will use commercially reasonable efforts to provide support to Customer as described in the Service Level Agreement. In the event that Customer earns 15 days of service credits, determined in accordance with the terms of the Service Level Agreement, in each of three consecutive months, Customer may notify Duo Security of its intention to terminate the Services and may terminate its Agreement with Duo Security for the provision of the Services to Customer and, as the sole and exclusive remedy, Customer will receive a refund of any pre-paid subscription Fees paid for Services not rendered as of the termination date.

2.5 Duo Security collects certain information about Customer and its Users as well as their respective devices, computers and use of the Services. Duo Security uses, discloses and protects this information as described in this Agreement and Duo Security's Privacy Policy (the "Privacy Policy") dated March 24, 2016, attached to this document as Appendix B.

### 3. CUSTOMER RESPONSIBILITIES

3.1 Customer may only use the Services in accordance with the Documentation and as explicitly set forth in this Agreement. Customer will cooperate with Duo Security in connection with the performance of this Agreement as may be necessary, which may include making available such personnel and information as may be reasonably required to provide the Services or support. Customer is solely responsible for determining whether the Services are sufficient for its purposes, including but not limited to, whether the Services satisfy Customer's legal and/or regulatory requirements.

3.2 Use of the Services may require Users to install Duo Mobile Software on their mobile devices. In addition, third party terms may apply with respect to third party products and software accessible via the Services and with respect to devices using third party operating systems or software or in the event that Duo Mobile Software is downloaded from third party sites (collectively, "Third Party Services"). Customer's access and use of Third Party Services is governed solely by the terms and conditions of such Third Party Services. Duo Security does not endorse, is not responsible or liable for, makes no representations or warranties and provides no indemnification with respect to any aspect of the Third Party Services, notwithstanding anything in this Agreement to the contrary. Duo Security is not liable for any damage or loss caused or alleged to be caused by or in connection with enablement, access or use of any such Third Party Services, or Customer's reliance on the privacy practices, data security processes or other policies of such Third Party Services. Duo Security does not provide customer support or assistance with respect to the Third Party Services. Users may be required to register for or log into such Third Party Services on their respective websites or apps.

3.3 Customer acknowledges that the Services will require the Users to share with Duo Security certain information for the purposes of providing the Services, such as user names, password and other login information. This information may include personal information (such as email address, and/or phone number) regarding the Users, and Duo Security will use such information for the purposes of providing the Services to Customer and Users. Prior to authorizing an individual to become a User, Customer is fully responsible for obtaining the consent of that individual, in accordance with all applicable laws, to the use of his/her information by Duo Security for purposes of providing the Services, which use shall be governed by the terms of the Privacy Policy. Customer represents and warrants that all such consents have been or will be obtained prior to authorizing any individual to become a User.

3.4 Customer will be fully responsible for Users' compliance with this Agreement. Any breach of this Agreement or such other terms by a User shall be deemed to be a breach by Customer. Customer is solely responsible for determining whether the Services are sufficient for Customer's purposes.

3.5 There will be no force or effect given to any different or additional terms contained in any purchase order or similar form issued by either party, even if signed by the parties after the date hereof unless such terms are included in an amendment in accordance with the terms of Section 14.3 of this Agreement. Each party's acceptance of this Agreement was and is expressly conditional upon the other's acceptance of the terms contained in the Agreement to the exclusion of all other terms.

### 4. RESTRICTIONS

Customer will not, and will not permit any of its Users nor any third party to: reverse engineer, decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas or algorithms of the Services, Software, Hardware Tokens or any data related to the Services (except to the extent such prohibition is contrary to applicable law that cannot be excluded by the agreement of the parties); modify, translate, or create derivative works based on the Services or Software; share, rent, lease, loan, resell, sublicense, distribute, use or otherwise transfer the Services or Software for timesharing or service bureau purposes or for any purpose other than its own use; or use the Services or Software other than in accordance with this Agreement and in compliance with all applicable laws and regulations (including but not limited to any European privacy laws and intellectual property laws).

### 5. PAYMENT OF FEES

5.1 Customer will pay the GSA MAS Contractor and the GSA MAS Contractor will pay Duo Security the Fees plus all applicable sales, use and other purchase related taxes (or provide Duo Security with a valid certificate of exemption from the requirement of paying sales, use or other purchase related taxes) in accordance with the Prompt Payment Act and the Order Form. Except as otherwise indicated in the applicable Order Form, all fees and expenses shall be in U.S. dollars. Duo Security will not charge users any fees for their use of the Services or Duo Mobile Software without Customer's authorization. Users' carriers or service providers may charge fees for data usage, messaging, phone calls or other services that are required for them to use the Services.

5.2 Customer's Order Form will indicate an initial allotment of Telephony Credits, if applicable. Customer may purchase additional Telephony Credits separately via the billing section of Customer's administrative interface or by contacting a sales representative. U.S. and international rates for telephony can be found at [https://www.duosecurity.com/docs/telephony\\_credits](https://www.duosecurity.com/docs/telephony_credits).

5.3 At any time during the Term, and unless otherwise agreed to in writing by the parties, any increase or overage in the maximum number of Users specified in the Order Form will be treated in accordance with this Section 5.3 (a "Subscription Upgrade"). The maximum number of Users shall be increased as follows:

For Subscription Upgrades (i) for Customers where the maximum number of Users on the Order Form is fewer than 500 Users, the maximum number of Users will be increased automatically in increments equal to 50 Users, (ii) for Customers where the maximum number of Users on the Order Form is 500 - 1000 Users, the maximum number of Users will be increased automatically in increments equal to 100 Users, and (ii) for Customers where the maximum number of Users on the Order Form is 1001 or greater, the maximum number of Users will be increased automatically in increments equal to 250 Users.

Duo Security shall invoice Customer for the increase in the maximum number of Users at the subscription rate and payment terms specified in the most recent Order Form, which will be prorated for the remainder of the then applicable subscription Term. For any future subscription Term, the number of Users and applicable Fees will reflect any Subscription Upgrades.

## 6. CONFIDENTIALITY

6.1 Each party (the "Receiving Party") understands that the other party (the "Disclosing Party") has disclosed or may disclose information relating to the Disclosing Party's technology, Users or business (hereinafter referred to as "Confidential Information" of the Disclosing Party).

6.2 The Receiving Party agrees: (i) not to disclose the Confidential Information to any third person other than those of its employees, investors and potential acquirers with a need to have access thereto and who have entered into non-disclosure and non-use agreements applicable to the Disclosing Party's Confidential Information or are subject to the Federal Trade Secrets Act (18 USC §1905), and (ii) to use such Confidential Information solely as reasonably required in connection with the Services and/or this Agreement. The Receiving Party further agrees to take the same security precautions to protect against unauthorized disclosure or unauthorized use of such Confidential Information of the Disclosing Party that the party takes with its own confidential or proprietary information, but in no event will a party apply less than commercially reasonable precautions to protect such Confidential Information. Each party acknowledges that the use of such precautions is not a guarantee against unauthorized disclosure or use. The Disclosing Party agrees that the foregoing will not apply with respect to any information that the Receiving Party can document (a) is or becomes generally available to the public without any action by, or involvement of, the Receiving Party, or (b) was in its possession without a duty of non-disclosure or known by it prior to receipt from the Disclosing Party, or (c) was rightfully disclosed to it without restriction by a third party, or (d) was independently developed without use of any Confidential Information of the Disclosing Party. Nothing in this Agreement will prevent the Receiving Party from disclosing the Confidential Information pursuant to any judicial or governmental order, provided that, to the extent permitted by law, the Receiving Party gives the Disclosing Party reasonable prior notice of such disclosure to contest such order. For the avoidance of doubt, Customer acknowledges that Duo Security utilizes the services of certain third parties in connection with the provision of the Services (such as data hosting and telephony service providers) and the provision of the Third Party Services and such third parties will have access to Customer's Confidential Information, subject to compliance with this Section 6. The parties agree that Performance Data and any other de-identified information in any form or format is not Confidential Information and will not be subject to any confidentiality restrictions or obligations.

6.3 Customer acknowledges that Duo Security does not wish to receive any Confidential Information from Customer that is not necessary for Duo Security to perform its obligations under this Agreement, and, unless the parties specifically agree otherwise, Duo Security may reasonably presume that any unrelated information received from Customer is not confidential or Confidential Information, unless such information is marked as "Confidential".

## 7. INTELLECTUAL PROPERTY RIGHTS; OWNERSHIP

Except as expressly set forth herein, Duo Security alone (and its licensors, where applicable) will retain all Intellectual Property Rights relating to the Services or the Software or any suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by Customer or any third party relating to the Services and/or the Software, which are hereby assigned to Duo Security. Customer will not copy, distribute, reproduce or use any of the foregoing except as expressly permitted under this Agreement. As between the parties, Duo Security will own all Performance Data, all other forms of aggregated information, and all de-identified data relating to any User and/or the Services. This Agreement is not a sale and does not convey to Customer any rights of ownership in or related to the Services or Software, or any Intellectual Property Rights.

**US Government Rights.** The Services and Software are "commercial items" as that term is defined at FAR 2.101. If Customer is the

US Federal Government (Government) Executive Agency (as defined in FAR 2.101), Duo Security provides the Services and Software, including any related technical data, and/or professional services in accordance with the following: If acquired by or on behalf of any Executive Agency (other than an agency within the Department of Defense (DoD), the Government acquires, in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Computer Software), only those rights in technical data and software customarily provided to the public as defined in this Agreement. If acquired by or on behalf of any Executive Agency within the DoD, the Government acquires, in accordance with DFARS 227.7202-3 (Rights in commercial computer software or commercial computer software documentation), only those rights in technical data and software customarily provided in this Agreement. In addition, DFARS 252.227-7015 (Technical Data – Commercial Items) applies to technical data acquired by DoD agencies. Any Federal Legislative or Judicial Agency shall obtain only those rights in technical data and software customarily provided to the public as defined in this Agreement. If any Federal Executive, Legislative, or Judicial Agency has a need for rights not conveyed under the terms described in this Section, it must negotiate with Duo Security to determine if there are acceptable terms for transferring such rights, and a mutually acceptable written addendum specifically conveying such rights must be included in any applicable contract or agreement to be effective. If this Agreement fails to meet the Government's needs or is inconsistent in any way with Federal law, and the parties cannot reach a mutual agreement on terms for this Agreement, the Government agrees to terminate its use of the Services and return the Software, unused, to Duo Security. This U.S. Government Rights clause in this Section is in lieu of, and supersedes, any other FAR, DFARS, or other clause, provision, or supplemental regulation that addresses Government rights in computer software or technical data under this Agreement.

## **8. DATA PROTECTION**

8.1 In this Section 8, the terms “personal data”, “data processor”, “data subject”, “process and processing” and “data controller” shall be as defined in the DPA.

8.2 For the purposes of the Data Protection Laws, as between Customer and Duo Security, the parties agree that Customer shall at all times be the data controller and Duo Security shall be the data processor with respect to the processing of Customer Personal Data in connection with this Agreement.

8.3 By entering into this Agreement, Customer agrees that Duo Security may collect, retain and use certain Customer Personal Data (which may include, without limitation, names, mobile telephone numbers, IP addresses and email addresses of Users) in connection with the Services. As the data controller of such Customer Personal Data, Customer shall be responsible for ensuring that, and warrants and represents to Duo Security that it shall ensure that any processing of Customer Personal Data in connection with the Services shall comply with the Data Protection Laws. This shall include (without limitation) ensuring that Customer: (a) has given adequate notice and made all appropriate disclosures to the data subjects regarding Customer's and/or Duo Security's use and disclosure of Customer Personal Data, including (but without limitation) for the provision of the Services; and (b) has and/or obtains all necessary rights, and where applicable, all appropriate and valid consents from the data subjects to share such personal data with Duo Security and to permit use of Customer Personal Data by Duo Security for the purposes of the provision of the Services and performing its obligations under this Agreement or as may be required by applicable law (“Purpose”), including (but without limitation) notifying the data subject of the transfer of Customer Data outside of the European Economic Area to countries whose laws they have acknowledged may provide a lower standard of data protection than exists in the European Economic Area (“EEA”).

8.4 At the request of Customer, Duo Security and Customer shall negotiate a separate data processing agreement, setting forth each Party's obligations in respect of any processing of Customer Personal Data, which agreement will be incorporated herein by reference once executed by the Parties.

8.5 Customer acknowledges that Duo Security is reliant on Customer for direction as to the extent to which Duo Security is entitled to use and process Customer Data. Consequently, Duo Security will not be liable for any claim brought by a data subject to the extent that such action or omission resulted directly from Customer's instructions. Customer undertakes to comply in all respects with any applicable laws, regulations, standards and guidelines applicable to personal data and shall use all reasonable endeavors to where possible anonymize personal data sent to Duo Security.

## **9. INDEMNIFICATION.**

For Customers enrolled in one of the editions of Services requiring purchase, Duo Security shall indemnify and hold Customer harmless from liability to third parties resulting from infringement by the Services of any United States or United Kingdom patent or any copyright or misappropriation of any trade secret, provided Duo Security is promptly notified of any and all threats, claims and proceedings related thereto and given reasonable assistance and the opportunity (subject to the requirements of 28 USC §516, if applicable) to assume sole control over defense and settlement; Duo Security will not be responsible for any settlement it does not approve. The foregoing obligations do not apply with respect to portions or components of the Services (i) not created by Duo Security, (ii) resulting in whole or in part from Customer specifications, (iii) that are modified after delivery by Duo Security,

(iv) combined with other products, processes or materials where the alleged infringement relates to such combination, (v) where Customer continues allegedly infringing activity after being notified thereof or after being informed of modifications that would have avoided the alleged infringement, or (vi) where Customer's use of Services is not strictly in accordance with this Agreement and all related Documentation. If Duo Security receives information about an actual or alleged infringement or misappropriation claim that would be subject to indemnification rights set forth in this Section 9, Duo Security shall have the option, at its expense, to (i) modify the Software to be non-infringing; or (ii) obtain for Customer a license to continue using the Software. If Duo Security determines it is not commercially reasonable to perform either of the above options, then Duo Security may at its option elect to terminate the license for the Services and refund the unearned portion of any pre-paid subscription Fees, pro-rated on a monthly basis. THIS SECTION STATES CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR INFRINGEMENT, MISAPPROPRIATION AND/OR CLAIMS ALLEGING INFRINGEMENT OR MISAPPROPRIATION.

## **10. TERM; TERMINATION**

10.1 Subject to earlier termination as expressly provided for in this Agreement, the initial Term of this Agreement shall be for the Term specified in the Order Form, or in the event of multiple Order Forms, until the Term of all Order Forms has expired. Each Order Form and this Agreement shall terminate upon expiration or termination in accordance with this Section 10 unless Customer provides at least forty-five (45) days prior written notice to Duo Security that it wishes to renew by placing an order directly with Duo Security or renews the Services through GSA MAS contract. The Fees per User for each renewal Term will be in accordance with the GSA MAS contract or, if renewed directly with Duo Security, equal to the Fees per User for the immediately prior Term plus a price increase to be agreed upon by Duo Security and Customer. Any pricing increase will not exceed seven percent (7%) per year, unless the pricing was designated in the applicable Order Form as promotional or one-time; provided, however, the Fees for each renewal Term shall not exceed the list price as of the start date of such renewal Term.

10.2 In the event of any material breach of this Agreement, the GSA MAS Contractor, on behalf of Duo Security, shall pursue its rights under the Contract Disputes Act or other applicable Federal statute while continuing performance as set forth in GSAR 552.212-4(d).

10.3 The Sections of this Agreement which by their nature should survive termination or expiration of this Agreement, including but not limited to Sections 3.1 and 4 through 14 (inclusive), will survive termination or expiration of this Agreement. No refund of Fees shall be due in any amount on account of termination by Duo Security pursuant to this Section 10. In the event of termination by Customer pursuant to this Section 10, Customer shall be entitled as its sole and exclusive remedy, to receive a refund of any pre-paid subscription Fees paid by Customer to Duo Security for Services not rendered as of the termination date. When this Agreement expires or terminates, Duo Security shall cease providing the Service to Customer.

## **11. WARRANTIES AND DISCLAIMER OF ADDITIONAL WARRANTIES**

11.1 For Customers enrolled in one of the editions of Services requiring purchase, Duo Security represents and warrants that it will not knowingly include, in any Duo Security software released to Users and provided to Customer hereunder, any computer code or other computer instructions, devices or techniques, including without limitation those known as disabling devices, trojans, or time bombs, that intentionally disrupt, disable, harm, infect, defraud, damage, or otherwise impede in any manner, the operation of a network, computer program or computer system or any component thereof, including its security or User data. If, at any time, Duo Security fails to comply with the warranty in this Section 11.1, Customer may promptly notify Duo Security in writing of any such noncompliance. Duo Security will, within thirty (30) days of receipt of such written notification, either correct the noncompliance or provide Customer with a plan for correcting the noncompliance. If the noncompliance is not corrected or if a reasonably acceptable plan for correcting them is not established during such period, Customer may terminate this Agreement and receive a refund of any pre-paid but unearned subscription Fees, pro-rated on a monthly basis, as its sole and exclusive remedy for such noncompliance.

11.2 For Customers that have purchased Hardware Tokens as part of the Services, Duo Security warrants to Customer only that Hardware Tokens will be free of defects in material and workmanship at the time of sale and for a period of six (6) months thereafter. This limited warranty is limited to replacement of defective Hardware Tokens. This limited Hardware Token warranty is Customer's exclusive remedy for defective Hardware Tokens.

11.3 EXCEPT FOR THE EXPRESS WARRANTIES PROVIDED IN THIS SECTION 11, THE SERVICES AND DUO SECURITY CONFIDENTIAL INFORMATION AND ANYTHING PROVIDED IN CONNECTION WITH THIS AGREEMENT ARE PROVIDED "AS-IS," WITHOUT ANY WARRANTIES OF ANY KIND. DUO SECURITY HEREBY DISCLAIMS FOR ITSELF AND ITS SUPPLIERS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ALL IMPLIED WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PURPOSE OR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, TITLE, AND NON-INFRINGEMENT.

## **12. LIMITATION OF LIABILITY**

12.1 NOTHING IN THIS AGREEMENT (OR ANY ORDER FORM) SHALL LIMIT OR EXCLUDE EITHER PARTY'S LIABILITY FOR (A) DEATH OR PERSONAL INJURY CAUSED BY ITS NEGLIGENCE, OR THE NEGLIGENCE OF ITS EMPLOYEES, AGENTS OR SUBCONTRACTORS; (B) FRAUD OR FRAUDULENT MISREPRESENTATION; OR (C) ANY OTHER LIABILITY THAT CANNOT BE EXCLUDED OR LIMITED BY LAW.

12.2 SUBJECT TO SECTION 12.1, IN NO EVENT WILL DUO SECURITY OR ITS SUPPLIERS BE LIABLE TO CUSTOMER (OR ANY PERSON CLAIMING UNDER OR THROUGH CUSTOMER) FOR ANY INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN ANY WAY CONNECTED WITH THE USE OF THE SERVICES OR ANYTHING PROVIDED IN CONNECTION WITH THIS AGREEMENT, THE DELAY OR INABILITY TO USE THE SERVICES OR ANYTHING PROVIDED IN CONNECTION WITH THIS AGREEMENT OR OTHERWISE ARISING FROM THIS AGREEMENT, INCLUDING WITHOUT LIMITATION, (I) LOSS OF REVENUE OR ANTICIPATED PROFITS (WHETHER DIRECT OR INDIRECT) OR (II) LOST BUSINESS OR (III) LOST SALES, WHETHER BASED IN CONTRACT, TORT (INCLUDING ACTIVE AND PASSIVE NEGLIGENCE AND STRICT LIABILITY) BREACH OF STATUTORY DUTY OR OTHERWISE, EVEN IF DUO SECURITY HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES.

12.3 SUBJECT TO SECTION 12.1, THE TOTAL LIABILITY OF DUO SECURITY FOR ANY CLAIM, WHETHER BASED IN CONTRACT, TORT (INCLUDING ACTIVE AND PASSIVE NEGLIGENCE AND STRICT LIABILITY) OR OTHERWISE, WILL NOT EXCEED, IN THE AGGREGATE, THE FEES PAID OR TO BE PAID TO DUO SECURITY HEREUNDER IN THE TWELVE MONTH PERIOD ENDING ON THE DATE THAT SUCH CLAIM IS FIRST ASSERTED, PROVIDED, HOWEVER THAT THE MAXIMUM LIABILITY OF DUO SECURITY FOR ALL CLAIMS SHALL BE THE THEN CURRENT ANNUALIZED VALUE OF THE APPLICABLE ORDER FORM. THE FOREGOING LIMITATIONS WILL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

### 13. U.S. GOVERNMENT MATTERS

Notwithstanding anything else, Customer may not provide to any person or export or re-export or allow the export or re-export of the Services or any software or anything related thereto or any direct product thereof, in violation of any restrictions, laws or regulations of the United States Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, or any other United States or foreign agency or authority.

### 14. MISCELLANEOUS

14.1 Severability. If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable.

14.2 Assignment. This Agreement is not assignable, transferable or sublicensable by either party except with the other party's prior written consent, which shall not be unreasonably withheld. This Agreement shall be binding upon and shall inure to the benefit of the parties hereto and their respective permitted successors and permitted assigns.

14.3 Entire Agreement; Amendment. Both parties agree that this Agreement and the GSA MAS Contract into which the Agreement is incorporated is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements, communications and other understandings relating to the subject matter of this Agreement, and that all waivers, amendments and modifications must be in a writing signed by both parties and specifically reference the provision of this Agreement being waived, amended or modified, except as otherwise provided herein. No agency, partnership, joint venture, or employment is created as a result of this Agreement and Customer does not have any authority of any kind to bind Duo Security in any respect whatsoever.

14.4 Notices. All notices under this Agreement will be in writing and will be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by facsimile or e-mail; and upon receipt, if sent by certified or registered mail (return receipt requested), postage prepaid. Duo Security may provide notice using the information provided in the most recent Order Form and Customer may provide notice using the contact information provided on [duosecurity.com](http://duosecurity.com).

14.5 Force Majeure. Any delay or failure in the performance of any duties or obligations of either party (except the payment of money owed) will not be considered a breach of this Agreement if such delay or failure is due to a labor dispute, fire, earthquake, flood or any other event beyond the reasonable control of a party, provided that such party promptly notifies the other party thereof and uses reasonable efforts to resume performance as soon as possible.

14.6 Governing Law; Arbitration. This Agreement will be governed by the Federal law.

14.7 Publicity. Upon the Customer's prior written consent, Duo Security may mention Customer's name in press announcements, case studies, trade shows, or other marketing or advertising materials.



Appendix A  
Service Level Agreement

**Duo Security SLA** During the term of your Duo Security license (the “Agreement”, the Duo web admin interface and web services will be operational and available to Customer at least 99.9% of the time in any calendar month (the “Duo Security SLA”). If Duo Security does not meet the Duo Security SLA, and if Customer meets its obligations under this Duo Security SLA, Customer will be eligible to receive the Service Credits described below. This Duo Security SLA states Customer’s sole and exclusive remedy for any failure by Duo Security to meet the Duo Security SLA.

**Definitions** The following definitions shall apply to the Duo Security SLA.

- “Downtime” means when there is more than a five percent user error rate across all of a Customer’s users. Downtime is measured based on server side error rate.
- “Service” means the Duo Security multifactor authentication service.
- “Monthly Uptime Percentage” means total number of minutes in a calendar month minus the number of minutes of Downtime suffered in a calendar month, divided by the total number of minutes in a calendar month.
- “Service Credit” means the number of days of Service to be added to the end of the Service term, at no charge to Customer calculated as follows:

Uptime	Days Credited
< 99.9% - ≤ 99.0%	3
< 99.0% - ≤ 95.0%	7
< 95.0%	15

**Customer Must Request Service Credit** In order to receive any of the Service Credits described above, Customer must notify Duo Security within thirty days from the time Customer becomes eligible to receive a Service Credit. Failure to comply with this requirement will forfeit Customer’s right to receive a Service Credit. Customer may check whether Duo Security’s systems are operational by visiting <https://status.duo.com>.

**Maximum Service Credit** The aggregate maximum number of Service Credits to be issued by Duo Security to Customer for all Downtime that occurs in a single calendar month shall not exceed fifteen days of Service (or the value of 15 days of Service in the form of a monetary credit to a monthly-billing Customer’s account). Service Credits may not be exchanged for, or converted to, monetary amounts.

**Duo Security SLA Exclusions** The Duo Security SLA does not apply to any services that expressly exclude this Duo Security SLA (as stated in the documentation for such services) or any performance issues: (i) caused by “Force Majeure” or (ii) that resulted from one or more of Customer’s equipment or third party equipment not within the primary control of Duo Security.

*Duo Security reserves the right to modify this Service Level Agreement at any time by updating the terms on*

*<https://www.duo.com/legal/sla>.*

# Privacy Policy

Last updated: March 24, 2016

## Who We Are

Duo Security, Inc. is a company incorporated under the laws of the State of Delaware, USA and whose principal office is located at 123 North Ashley Street, Suite #200, Ann Arbor, Michigan 48104, USA.

In this Privacy Policy when we refer to “**Duo Security**” or “**we**”, “**us**” or “**our**”, we mean either Duo Security Inc. or the relevant Duo Security group company which provides you with our services and mobile and web-based applications, (including Duo Security UK Limited) as more completely described on our Website (collectively, the “**Services**”). Duo Security is committed to protecting the privacy of individuals who visit our websites, including, but not limited to <https://www.duo.com> (collectively, the “**Website**”) and the customers and users of our services and mobile and web-based applications.

Terms not otherwise defined in this Privacy Policy have the meanings assigned to them in Duo Security’s Service Terms and Conditions. When you access and use the Services, the Service Terms and Conditions and this Privacy Policy apply.

If you have any questions about how we collect, store and use personal information, or if you have any other privacy-related questions, please contact us by any of the following means:

By post: Duo Security, Inc., 123 North Ashley Street, Suite #200, Ann Arbor, MI 48104, USA

By facsimile: 1-866-760-4247

By email: [security@duosecurity.com](mailto:security@duosecurity.com)

## Introduction

This Privacy Policy describes how we collect, use, share and transfer Personal Information (as defined below) created, inputted, submitted, posted, transmitted, stored or displayed by individuals who interact with and use the Duo Security Website and Services. This Privacy Policy does not apply to Personal Information (as defined below) we obtain in our capacity as an employer; employment related data is covered under separate policies and/or notices. This Privacy Policy covers information we collect online, not offline.

Any Personal Information we collect through the Services will be used only in a manner consistent with this Privacy Policy. When you sign up for or access the Services, including blog updates or newsletters, or when you email us for information, you expressly agree to the use of your information for the purposes described in this Privacy Policy. If you do not agree with the use of personal information as described in this Privacy Policy or any changes to it, you should not sign up for, use or access the Services or any features of the Services.

## Changes to Our Privacy Policy

We may revise this Privacy Policy from time to time. The most current version of this Privacy Policy will govern your use of your Personal Information. If we decide to change our Privacy Policy, we will post the updated Privacy Policy on the Website and update the Privacy Policy modification date. Please check back regularly to review any changes to this Privacy Policy. By continuing to use the Service after those changes become effective, you agree to be bound by the revised Privacy Policy.

## Personal Information

“**Personal Information**” is defined slightly differently across the world, but we define “Personal Information” as any information that could be used to identify you or another individual, such as (but not limited to) an individual’s name, email address, or telephone number, and that is not otherwise publicly available. Personal Information may include other types of information as well, such as some of the information referred to under the subheadings “**Device-Specific Information**” and “**Service Log Information.**”

We also collect non-personal information that does not, on its own, identify any individual person. When non-personal information is combined with other information so that it does identify an individual person, we treat that information as Personal Information.

## What Information do we collect?

When you use the Services we may collect, store and process certain information about you, including:

### Contact Information.

Duo Security may collect, store and process the following contact information in order to provide the Services:

**For Organization Users:** If your user profile is created by or at the request of an organization (an “**Organization**”) of which you are an employee, contractor, member, agent or other participant (each such user referred to as an “**Organization User**”) your “**Organization’s Administrator**” may provide us with certain Personal Information, such as your name, email address, and telephone number. We also collect your Organization name and assign you an account name based on your Organization name. Prior to authorizing you to become a user of the Services, your Organization is responsible for notifying you and/or obtaining your consent to the collection of such information, in accordance with applicable laws. Even though your Organization has notified you and/or received your consent to provide us with your Personal Information, when you begin using the Services, you are also providing your consent

to the terms in this Privacy Policy and our Service Terms and Conditions.

- **For Personal Edition Users:** If you establish a “Personal Edition” account (as compared to an Organization account), and/or if you sign up for our newsletters and email updates we may collect your name, email address, and telephone number.
- **For Organization Administrators:** for each Organization account we may collect the name, email address, and telephone number of any Organization Administrators, or similar points of contact, within the Organization in order to be able to provide you and the Organization with the Services and to manage your account.

We also collect your email address when you email us for information or sign up for our newsletters and email updates. You can unsubscribe from our newsletters and updates by clicking “Unsubscribe” at the bottom of the newsletter or email update or by emailing [mops@duosecurity.com](mailto:mops@duosecurity.com).

**Public Forums:** We collect other information, including Personal Information that you submit to our Website or as you participate in certain interactive features of our Services (such as the publicly accessible blogs or community forums). You should be aware that any information (including Personal Information) you provide in these areas may be read, collected, and used by others who access them. To request removal of your Personal Information from our blog or community forum, contact us at [security@duosecurity.com](mailto:security@duosecurity.com). In some cases, we may not be able to remove your Personal Information, in which case we will let you know if we are unable to do so and why.

**Testimonials/Reviews/Feedback:** We may post customer testimonials on our Website, which may contain Personal Information. We do obtain the customer’s consent via email prior to posting the testimonial to post their name along with their testimonial. If you want your testimonial removed, please contact us at [security@duosecurity.com](mailto:security@duosecurity.com).

**Surveys:** We may provide you the opportunity to participate in contests or surveys. If you participate, we will request and collect certain Personal Information from you at the time of the survey. Participation in these surveys or contests is completely voluntary and you have a choice whether or not to disclose this information. The requested information typically includes contact information, such as email or phone number.

When you use the Service we may collect, store and process certain information collected by us from your web browser or from interactions with the Services, including:

**Device-Specific Information.** We also collect device-specific information (e.g. mobile and desktop) from you in order to provide the Services. Device-specific information includes:

- attributes (e.g. hardware model, operating system, web browser version, as well as unique device identifiers and characteristics (such as, whether your device is “jailbroken,” whether you have a screen lock in place and whether your device has full disk encryption enabled));
- connection information (e.g. name of your mobile operator or ISP, browser type, language and time zone, and mobile phone number); and
- device locations (e.g. internet protocol addresses and Wi-Fi).

We may need to associate your device-specific information with your Personal Information on a periodic basis in order to confirm you as a user and to check the security on your device.

**Service Log Information.** When you use the Services, we may automatically collect and store certain information in server logs. This may include which users (by reference to certain Personal Information such as the user’s: username; email address; name; and other information that may be included in open textual fields) are accessing the Services, how users are accessing the Services (including the device-specific information referenced above and type of integration (i.e. application) being protected), the dates and times you are accessing the Services, from where you are accessing the Services (by internet protocol address) and device event information such as crashes, system activity, and hardware settings. We may need to associate this information with other information we collect about you on a periodic basis in order to confirm you as a user and to check the security on your device. We may also do this to improve the Services that we offer you.

**Social Media Widgets:** Our website includes plugins of social media platforms, such as facebook.com of Facebook Inc., 1601 S. California Ave, Palo Alto, CA 94304, USA; Twitter.com of Twitter Inc., 795 Folsom St., Suite 600, San Francisco CA 94107, USA; and google+ of Google Inc., 1600 Amphitheatre Parkway Mountain View, California, 94043, USA. Social Media Features and Widgets are either hosted by a third party or hosted directly on our websites.

- You can generally identify the plugins by the respective network’s logo, for instance in combination with a pictogram of a clenched hand with a raised thumb or the addition of a “recommendation”, “like” or “comment.”

Details about purpose and extent of data collection as well as processing and usage of the data by the social media networks can be obtained by reading the privacy policies of Facebook [<http://www.facebook.com/policy.php>], Twitter [<http://twitter.com/privacy>] and Google [<https://www.google.com/policies/privacy/>].

## How do we use the Information We Collect?

Information we collect may be used for the following purposes:

- to provide the Services;
- for billing purposes;
- to personalize the Services and improve your experience;
- improving our products, technology and services;
- for analytical purposes, including use of "**Performance Data**". Performance Data includes aggregate, de-identified usage information and other aggregate measures of the Services' performance. We may share aggregated, de-identified Performance Data with third parties to help us better understand our customers' needs and improve the Services;
- for marketing and advertising purposes, including sending you promotional email messages about our products and services and registering you for our events. If you do not want us to use your data in this way, please opt out here: <https://go.duosecurity.com/UnsubscribePage.html> or send an email to [mops@duosecurity.com](mailto:mops@duosecurity.com). For more information about how to change your preferences and to unsubscribe from promotional materials, then please see the section headed "Choice and Consent". Duo Security does not market or advertise to Organization Users;
- to prevent, detect, identify, investigate, respond and protect against potential or actual claims, liabilities, prohibited behavior, and criminal activity;
- to comply with and enforce applicable legal requirements, agreements and policies;
- to perform other activities consistent with this Privacy Policy;
- to improve the Services and where you have agreed, to provide you updates on how we are improving the Services based on any feedback you might have given; and
- with respect to Organization Users, to provide you and the Organization with the Services and to manage your account.

## Data Retention

The time periods for which we retain your Personal Information depend on the purposes for which we use it. We will retain your information for as long as your account is active or as needed to provide you the Services, unless we are required by law to dispose of it earlier or to keep it longer. We will also retain and use your information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements. Please contact us as provided in the Notice section below if you have any questions about the information we collect and/or how we use the information we collect.

## Sharing of Personal Information Collected

Duo Security does not sell, rent, or trade and, except as described in this Privacy Policy, does not share any Personal Information with third parties for their promotional purposes.

Duo Security may transmit or share Personal Information as follows:

- We may share Personal Information, with our authorized third party vendors, consultants, service providers and hosting partners (currently Amazon Web Services) who perform services for Duo Security (including hardware, software, networking, storage, and other technology and services required to operate, maintain and provide support related to the Services) based on Duo Security's instructions. These third parties may only use or disclose such Personal Information obtained from Duo Security to perform the Services on Duo Security's behalf or comply with legal obligations.
- If you have an Organization account, we may also share Personal Information and/or Device-Specific Information with your Organization and/or your Organization's third party vendors (with your employer's consent) in order to operate and maintain the Services. Your device may be subject to your Organization's policies and practices, which are separate from this Privacy Policy. We have no control over your Organization and your Organization's third party vendors' privacy practices, so please read their applicable privacy policies. Our Privacy Policy does not apply to, and Duo Security is not responsible for, use of your Personal Information by these other companies.
- We may share your Personal Information with third parties to send emails on our behalf, and/or for co-branded and/or co-sponsored marketing and promotional events (such as conference events) offered in conjunction with another company or companies. If you register for or participate in such marketing and promotional events, both Duo Security and such other companies may receive information collected in conjunction with the co-branded and/or co-sponsored marketing and promotional events. Our Privacy Policy will apply to you with respect to our use of your Personal Information. We have no control over any other companies' privacy practices, so please read their applicable privacy policies before providing any Personal Information. Our Privacy Policy does not apply to, and Duo Security is not responsible for, use of your Personal Information by these other companies.
- Duo Security may share information internally with other members of the Duo Security family of companies, including Duo Security UK Limited (a company registered in England and Wales) for the purposes described in this Privacy Policy.
- We may also disclose Personal Information; (i) if we are required to do so by law or legal process; (ii) to respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims; (iii) as may be required for the purposes of national security; (iv) when we believe disclosure is necessary and appropriate to prevent physical, mental, financial or other harm, injury or loss; or (v) in connection with an investigation of suspect or actual illegal or inappropriate activity or exposure to liability. We may also share such information if we believe it is necessary in order to investigate, prevent, or



take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of our Service Terms and Conditions and any other agreements, or as otherwise required by law or to comply with any legal obligation.

When we share Personal Information with a third party, they must contractually agree to comply with privacy and security standards at least as stringent as Duo Security's when it is handling similar data. When you provide data directly to the third party, the processing is based on their standards (which may or may not be the same as Duo Security's) and your own independent relationship with that provider.

By accessing, signing up for or using the Services, sending us email, or by signing up for email updates, you provide your express consent to our disclosure of your Personal Information to our third party service providers (such as credit card processors, managed hosting service providers, sub-processors of service data, and technology partners) in order to supply our Services. We do not permit our service providers to use your Personal Information for their own marketing purposes or for any other purpose than in connection with the services they provide to us.

## **Credit Card Information**

Some of our customers use credit cards, debit cards or other means to pay for our Services. We do not collect credit card, debit card or personal financial account information through our Website. We use a third party vendor, currently Recurly, Inc., to process our subscription billing. When you provide payment information to pay for the Services, you provide it directly to Recurly, and not to Duo Security. You will automatically be routed to the Recurly website to provide the information Recurly requires to process your transaction. Recurly is a third party vendor and has its own privacy policy, which may be different from this Privacy Policy. This Privacy Policy does not cover information collected by Recurly and Duo Security is not covered by, or responsible for, Recurly's privacy practices or policy. To learn about Recurly's privacy practices, please read their privacy policy at <http://recurly.com/legal/privacy>.

## **Accessing and Updating Your Personal Information**

You can modify your account information at any time by using the Service administrative interface available at <https://admin.duosecurity.com> or by emailing our customer support at [support@duosecurity.com](mailto:support@duosecurity.com). We will respond to your request to access promptly and within no more than 30 days.

## **Cookies and other Tracking Technologies**

When you visit our Website or use our Services, we use "cookies" and other tracking technologies like "web beacons" to allow us to remember your user preferences, to maximize the performance of our Website and Services, enhance and personalize your experience and provide marketing communications. They also help ensure that

advertisements you see while you are on our Website are more relevant to your interests.

**For further information about cookies and the other tracking technologies we use, along with information about how to disable or block cookies, please see our Cookie Policy at <https://www.duo.com/legal/cookies>.**

## Security of Information

Duo Security maintains and uses reasonable administrative, organizational, technical and physical safeguards to protect your information from loss, destruction, misuse, unauthorized access or disclosure as required by applicable law. These technologies help ensure that your data is safe, secure, and only available to you and to those you provided authorized access (e.g., your users). For example, when you enter confidential information (such as login credentials or information submitted from within the Service), we encrypt the transmission of that information using secure socket layer technology (SSL). SSL technology is designed to prevent you from inadvertently revealing personal information using an insecure connection. However, no electronic transmission over the Internet or information storage technology can be guaranteed to be 100% secure, so you should take care in deciding what information you send us in this way. If you have any questions about security on our Website, you can contact us at [security@duosecurity.com](mailto:security@duosecurity.com).

## Links to Other Sites

Our Website may contain links to other sites that are not owned or controlled by Duo Security. Please be aware that Duo Security is not responsible for the privacy practices of these other sites. We encourage you to review the privacy policies and statements of other sites to understand their information practices. Our Privacy Policy applies only to information collected by our Website and Services.

## Choice and Consent

We offer certain choices about how we communicate with our users and what Personal Information we obtain from them.

- You can opt out of receiving promotional emails or text messages from us by clicking the “unsubscribe” link in the email or by emailing [mops@duosecurity.com](mailto:mops@duosecurity.com);
- Many Duo Security products contain settings that allow users or administrators to control how the products collect information. Please refer to the relevant product documentation or contact us through the appropriate technical support channel for assistance.
- To remove your Personal Information from a Duo Security website testimonial, please contact us at [security@duosecurity.com](mailto:security@duosecurity.com).

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

## **Cross-Border Transfer of Your Personal Information**

Please be aware that Duo Security may host and process your data and information (including Personal Information), in the United States and other countries through the Duo Security group of companies and third parties that we use to operate and manage the Website and Services, including Amazon Web Services (“AWS”). You may view the AWS privacy policy at <http://aws.amazon.com/privacy>. By signing up for or using the Services, and/or by communicating with us by email, you acknowledge and expressly consent to the transfer and processing of your Personal Information in this way. Any such transfer or processing of your Personal Information will be in accordance with all applicable laws.

## **Your controls and choices**

You may request and obtain from us once a year, free of charge, certain information about the Personal Information (if any) we disclosed to third parties for direct marketing purposes in the preceding calendar year. If applicable, this information would include a list of the categories of Personal Information that was shared and the names and addresses of all third parties with which we shared information in the immediately preceding calendar year. If you would like to make such a request, please submit your request in writing as follows:

By post: Duo Security, Inc., 123 North Ashley Street, Suite #200, Ann Arbor, MI 48104, USA

By facsimile: 1-866-760-4247

By email: [security@duosecurity.com](mailto:security@duosecurity.com)

In addition, we currently do not honor Do Not Track signals.

## **Children’s Online Privacy Protection Act Compliance**

We are in compliance with the requirements of COPPA (Children’s Online Privacy Protection Act), as we do not collect any information from anyone under 13 years of age. The Website and its content are directed to people who are at least 18 years of age or older.

## **Children**

We do not collect any information from anyone under 18 years of age. The Website and its content are directed to people who are at least 18 years of age or older. If you are under the age of 18, you may not use this Website unless you have the consent of, and are supervised by, a parent or guardian.

## **Access to Your Information**

You have a right to access, review, change, update or delete your Personal Information at any time by contacting us at [security@duosecurity.com](mailto:security@duosecurity.com) or by postal mail at Duo Security, Inc., 123 North Ashley Street, Suite #200, Ann Arbor, MI 48104, USA. Please note that we may impose a small fee for access and disclosure of your Personal Information where permitted under applicable law, which will be communicated to you. We do not charge you to update or remove your Personal Information.

## **Contact Us**

Duo Security commits to resolving complaints about your privacy and our collection or use of your Personal Information. If you need to provide a Notice to us under this Privacy Policy or if you have complaints about our compliance with this Privacy Policy, you should first contact us as follows:

Ann Arbor, MI 48104, USA	By post: Duo Security, Inc., 123 North Ashley Street, Suite #200,
	By facsimile: 1-866-760-4247
	By email: <a href="mailto:security@duosecurity.com">security@duosecurity.com</a>

## **Business Transactions**

Duo Security may assign or transfer this Privacy Policy, and your user account and related information and data, to any person or entity that acquires or is merged with Duo Security.

# **Cookie Policy**

Last updated: March 24, 2016

The Website and/or Services use cookies to distinguish you from other users of our Website. This helps us provide you with a good experience when you browse the Website and also allows us to improve our Website.

This cookie policy provides you with information about the cookies we use and the purposes for using them. To review the privacy policies that apply to users of duo.com, please read our Privacy Policy at <https://www.duo.com/legal/privacy>. For further information about this policy, please contact [privacy@duosecurity.com](mailto:privacy@duosecurity.com).

## What Is A Cookie?

A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your computer or other device. Cookies send data back to the originating website on each subsequent visit, or share data with another website that recognizes that cookie. Unless you have adjusted your browser setting so that it will refuse cookies, our system will issue cookies as soon as you visit our Website or use the Services.

Cookies are useful because they allow a website to recognize a user's device. They do lots of different jobs, like letting you navigate between pages efficiently, remembering your preferences, and generally improving the user experience. They can also help to ensure that the advertisements you see online are more relevant to you and your interests.

Cookies do not typically identify you as an individual, just the device you are using. For further information on cookies, including how to see what cookies have been set on your device and how to manage and delete them see the section below headed "Information About Cookies".

## What Cookies Do We Use And Why?

When you visit our Website or use our Services, we use cookies, web beacons and other technologies for a variety of purposes, such as, to allow us to remember your user preferences; to maximize and analyze the performance of our Website and Services; and to analyze our performance. We also use cookies to provide, enhance and personalize certain aspects of the Services. Cookies are also used for targeting purposes as described below.

There are four different types of cookies we use:

- **Essential cookies.** These are cookies that are required for the operation of our Services. For example, when you download certain online technologies, a cookie is set that identifies the software, version, and when it expires. We may use this information to alert you that a newer version of such software is available and/or if your subscription is going to expire. These cookies are necessary for the Services to operate properly. Without these cookies, services that you have asked for cannot be provided. We want you to understand these essential cookies, and why we use them, but we don't need to get your consent to use them on our Services as we use these cookies only to provide you with services that you have requested.
- **Functionality cookies.** These cookies allow our Services to remember choices you make, such as: remembering your username, preferences and settings; remembering if you've filled in a survey or taken part in a poll or contest or otherwise reacted to

something on or through the Services, so you're not asked to do it again; remembering if you've used any of our Services before; restricting the number of time you are shown a particular advertisement; remembering your location; and enabling social media components like Facebook or Twitter. The aim of these cookies is to provide you with a more personal experience so that you don't have to reset your preferences each time you use our Services. We also use functionality cookies to enable you to comment on an article or provide enhanced services such as enabling you to view a video through the Services. As described below, you may disable any of these functional cookies; but if you do so, then various functions of our Services may be unavailable to you or may not work the way you want them to.

- **Analytical/Customization cookies.** These cookies collect information about how visitors use and interact with our Services, for instance which pages they go to most often. These cookies also enable us to personalize content, greet you by name, and remember your preferences (e.g., your choice of language, country, or region). These cookies help us improve the way our websites work and provide a better, personalized user experience. Some of our analytical/customization cookies are managed for us by third parties. However, we don't allow the third party to use the cookies for any purpose other than those listed above.
- **Advertising/ targeting cookies.** These cookies record your visit to our websites, the pages you have visited, and the links you have clicked. They gather information about your browsing habits and remember that you have visited a website. We (and third-party advertising platforms or networks) may use this information to make our websites, content, and advertisements displayed on them more relevant to your interests (this is sometimes called "behavioral" or "targeted" advertising). These types of cookies are also used to limit the number of times you see an advertisement as well as to help measure the effectiveness of advertising campaigns.

To find out more about interest-based ads and your choices, visit these sites: Digital Advertising Alliance, the Network Advertising Initiative, and the Interactive Advertising Bureau (IAB) Europe and these links: <http://www.allaboutcookies.org> or <http://www.youronlinechoices.com>.

## What Specific Cookies Do We Use In the Website and the Services?

Some of the cookies we commonly use are listed in our cookies chart below. This list is not exhaustive, but it is intended to illustrate primary reasons for certain types of cookies set by Duo Security and third parties on our Website and Services. Third parties may also set certain cookies on your device when you use our Services. In some cases, the third party has been hired to provide certain services on Duo Security's behalf (e.g., website analytics).

Service	Purpose	Cookie Name	Duration	Strictly Necessary	Category
Google Analytics	Web analytics	__utma	2 years	No	Analytics/Customization
		__utmb	1 day	No	Analytics/Customization

					tomization
		__utmc	Session	No	Analytics/ Customizat ion
		__utmz	6 months	No	Analytics/Cus tomization
		_ga	2 years	No	Analytics/Cus tomization
		_gat	1 day	No	Analytics/Cus tomization
Olark	Live chat	_ok	Session	No	Functionality
		_okbk	Session	No	Functionality
		_oklv	Session	No	Functionality
		hblid	2 years	No	Functionality
		okfsk	2 years	No	Functionality
		wcsid	Session	No	Functionality
Optimizely	A/B testing	optimizelyBuckets	10 years	No	Functionality
		optimizelyEnabledUserId	10 years	No	Functionality
		optimizelyPen	1 day	No	Functionality

		dingLogEvents			
		optimizelySegments	10 years	No	Functionality
Shareaholic	Content sharing	apq	5 years	No	Functionality
		kpq	5 years	No	Functionality
		rpq	5 years	No	Functionality
		p1	5 years	No	Functionality
		si	5 years	No	Functionality
		ss	5 years	No	Functionality
		gguuid	1 month	No	Functionality
AddThis	Content sharing	__atuvc	2 years	No	Functionality
		loc	2 years	No	Functionality
		uid	2 years	No	Functionality
		uit	1 day	No	Functionality
Wistia	Video hosting	__distillery	1 year	No	Functionality
Marketo	Marketing automation	_mkto_trk	2 years	No	Advertising / Targeting



		__cdrop	1 year	No	Advertising / Targeting
Duo	Trusted device feature	duo	1 day	No	Functionality
	Endpoint security				
	capability	trc xxxx yyyy	forever	No	Functionality
	Trusted device feature	fdc xxxx yyyy	Depends on admin config	No	Functionality

## Google Analytics

We use Google Analytics, a web analysis-tool of Google Inc., 1600 Amphitheatre Parkway Mountain View, California, 94043, USA, (“Google”). Google Analytics uses “cookies” to track visitor interactions, which are textfiles being saved to your computer to help us analyze visits of our Website and how our Services are used. For example, by using cookies, Google can tell us which pages our users view, which are most popular, what time of day our websites are visited, whether visitors have been to our websites before, what website referred the visitor to our websites, and other similar information.

For more information about Google analytic cookies, please see Google’s help pages and privacy policy:

Google Privacy Policy: <https://www.google.com/policies/privacy/>

Google Analytics Help: <https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage>

If you do not want your usage of our Website and Services to be analyzed by Google, you can disable Google Analytics by using an add-on in your Internet browser. You can download and install the add-on at: <https://tools.google.com/dlpage/gaoptout?hl=fr>.

## Google AdWords

We use Google AdWords Remarketing to advertise Duo Security. AdWords Remarketing will display relevant ads tailored to you based on what parts of the Duo Security website you have viewed by placing a cookie on your machine. This cookie does not identify you or give access to your computer. The cookie is used to identify you as a visitor to certain of our web pages and enables use to show you ads relating to that page. Google AdWords Remarketing allows us to tailor our marketing to better suit your needs and only display ads that are relevant to you.

If you do not wish to participate in our Google AdWords Remarketing, you can opt out by visiting [Google's Ads Preferences Manager](#).

You can also opt out of any third-party vendor's use of cookies by visiting <http://www.networkadvertising.org/choices/> or <http://www.youronlinechoices.com>. Another way to opt out is to use a Google browser plugin: <https://tools.google.com/dlpage/gaoptout/>

If you wish to opt-out of Google Advertising, you may visit <https://www.google.com/settings/ads> and under "Ads on Google" and/or under "Google Ads Across the Web," and click the "Opt out" link.

## Targeting

We give users the option to share our stories on social networks such as Facebook and Twitter. To deliver this service we link to the third party websites AddThis and Shareaholic. If you use our share buttons, you will be directed to a website controlled by AddThis and Shareaholic. We have no control over the cookies that AddThis and Shareaholic set when you use its services. You can opt out of AddThis cookies at <http://www.addthis.com/privacy/opt-out> and Shareaholic cookies at <https://shareaholic.com/privacy/choices>.

## Additional Third Party Cookies

We occasionally link to external websites or other third party content. If you click on external links, you will be directed to a website controlled by a third-party. We have no control over the cookies that the third-party sets when you use its service.

## How to Delete And Block Our Cookies

You can disable and/or delete cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies. However, if you use your browser settings to block all cookies (including essential cookies), you may not be able to access all or parts of our Website. Unless you have adjusted your browser setting so that it will refuse cookies, our system will issue cookies as soon as you visit our Website.

These settings are usually found in the "options" or "preferences" menu of your internet browser. In order to understand these settings, the following links may be helpful. Otherwise you should use the "Help" option in your Internet browser for more details.

The following links provide information on how to modify the cookie settings on some popular browsers.

Internet Explorer: <http://windows.microsoft.com/en-us/internet-explorer/delete-manage-cookies>

Firefox: <https://support.mozilla.org/en-US/kb/cookies-information-websites-store-on-your-computer>

Chrome: <https://www.google.com/policies/technologies/managing/>

Safari: <http://support.apple.com/kb/HT1677>

## Can I Withdraw My Consent?

If you wish to withdraw your consent at any time, you will need to delete your cookies using your Internet browser settings. For further information about deleting or blocking cookies, please visit: <http://www.aboutcookies.org> and <http://www.youronlinechoices.com>. While many companies involved in using advertising cookies and serving online behavioral advertising appear at the above links, not all do. Therefore, even if you choose to turn off cookies used by all of the companies listed, you may still receive some advertising cookies and some tailored advertisements from other companies.

You can also manage this type of cookie in the privacy settings on the web browser you are using. Please see above for more information.

## Your Consent

By continuing to use the Website or the Services, you are agreeing to our placing cookies on your computer or other device in order to analyze the way you use the Website and in order for us to provide the Services. Please read this cookie policy carefully for more details about the information we collect when you use this Website and the Services.

If you do not wish to accept cookies in connection with your use of this Website or Services, you must stop using our Website and Services.

## Information About Cookies

**All About Cookies:** Useful information about cookies can be found at: <http://www.allaboutcookies.org>

**Internet Advertising Bureau:** A guide to behavioral advertising and online privacy has been produced by the Internet advertising industry, which can be found at: <http://www.youronlinechoices.com>

## Our use of Web Beacons

We may also use electronic images known as web beacons on our Services - sometimes called “clear GIFs,” “single-pixel GIFs,” or “web bugs.” Web beacons are used to deliver cookies on our Services, count clicks/users/visitors, and deliver co-branded content or services. We may include web beacons in our promotional email messages or newsletters to determine whether messages have been opened and acted upon.

The Services may also contain web beacons from third parties to help us compile aggregated statistics regarding the effectiveness of our promotional campaigns or other website operations. These web beacons may allow the third parties to set or read cookies on your

device.

## **Other Similar Technologies**

In addition to the aforementioned cookies and web beacons, our Website also uses other technologies to store and retrieve data from your device. This may be done to maintain your preferences or to improve speed and performance by storing certain files locally.