FIGMA SOFTWARE SERVICES AGREEMENT

Effective Date: September 5, 2025

This Agreement is entered into between Figma and Customer, and governs Customer's access to and use of Figma offerings provided under Figma for Government plans. If Customer is purchasing through a Reseller, this Agreement supplements the agreement between Customer and Reseller governing the purchase of subscriptions to the Figma Platform. Capitalized terms used but not defined herein are defined in Exhibit A.

By accepting this Agreement as part of an Order, you agree to this Agreement on behalf of the entity for which you are acting (such as an employer) ("**Customer**"). You represent and warrant that you have full legal authority to bind Customer to this Agreement, and confirm Customer's agreement to be party to this binding contract. If you do not have the authority to bind Customer or do not agree with the terms of this Agreement, you (and Customer) are not authorized to access or use the Figma Platform.

1. **Figma Obligations**.

1.1. **Access to the Figma Platform**. Subject to the terms and conditions of this Agreement, Figma hereby grants Customer a limited, non-exclusive, non-transferable (subject to Section 9.6), non-sublicensable right in the Territory, during the Order Term, for Authorized Users to access and use the Figma Platform in connection with Customer's own business purposes.

1.2. **Protection of Customer Data**. Figma will implement and maintain the security requirements set forth in Exhibit B. The data processing addendum available at https://www.figma.com/dpa is hereby attached hereto and incorporated by reference.

2. **Service Terms**.

2.1. **Use Restrictions**. Except as otherwise expressly authorized in this Agreement, Customer will not, and will not encourage or assist third parties to: (i) reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code, object code, or underlying structure, ideas, know-how, or algorithms relevant to the Figma Platform (except to the extent such a restriction is impermissible under applicable law); (ii) provide, sell, resell, transfer, sublicense, lend, distribute, rent, or otherwise allow others to access or use the Figma Platform; (iii) copy, modify, create derivative works of, or remove proprietary notices from the Figma Platform; or (iv) use the Figma Platform for personal or other non-commercial purposes.

2.2. **Acceptable Use Policy**. Customer will comply with Figma's Acceptable Use Policy attached hereto and available at www.figma.com/aup/.

2.3. **Account Management**.

(a) As part of the registration process, Customer will appoint one or more administrative users for Customer's Figma account. Each administrative user has the authority to manage Customer's Figma account, add or remove Authorized Users, approve purchases, and otherwise act on behalf of Customer for purposes relating to the Figma Platform and this Agreement.

(b) Customer may enable Authorized Users to access and use the Figma Platform in accordance with the Documentation and any limitations in Customer's Order Form. Each Authorized User's account is personal to the Authorized User to which it is issued. Account credentials may not be shared or used by anyone other than the individual to whom they were provisioned. Customer is responsible for its Authorized Users' compliance with this Agreement, and all activities of its Authorized Users.

(c) Customer is responsible for providing accurate and complete account information (including the list of domains and/or Figma accounts owned or controlled by Customer for purposes of domain capture or migrations) and maintaining the accuracy and completeness of such information. Customer is responsible for maintaining control over its Authorized Users' accounts, including the confidentiality of usernames and passwords. Figma supports login using two-factor authentication ("**2FA**"), which is known to reduce the risk of unauthorized use of or access to the Figma Platform. Figma will not be responsible for any damages, losses, or liability to Customer, Authorized Users, or anyone else if any event leading to such damages, losses, or liability would have been prevented by the use of 2FA.

2.4 **Customer Content**. Customer authorizes Figma and its service providers to use Customer Content for the sole purpose of providing the Figma Platform and performing the activities contemplated by this Agreement (such as maintaining, securing, debugging, and otherwise performing quality control for the Figma Platform). Figma recognizes that the use of Customer Content for the purpose of training Artificial Intelligence/Machine Learning (AI/ML) models and systems is prohibited without explicit written authorization from the Federal agency contracting officer.

2.5. **Feedback**. Customer may voluntarily provide Figma feedback, comments, or suggestions concerning the Figma Platform or other services provided by Figma (collectively, "**Feedback**"). To the extent Customer provides Feedback, Customer hereby grants Figma the right to use such Feedback to maintain, improve, and enhance Figma's products and services.

2.6. **Usage Data**. Figma will have the right to collect and analyze data and other information relating to the access, use, and performance of the Figma Platform ("**Usage Data**") and Figma will be free (during and after the Order Term) to use Usage Data in de-identified and aggregated form to maintain, improve, and enhance Figma's products or services. Examples of Usage Data include technical logs, metadata, telemetry data, and usage information about Customer Content, such as how many times it is accessed. For clarity, Usage Data excludes Customer Content itself.

2.7. **Reservation of Rights**. As between the parties, Figma owns all right, title, and interest in the Figma Platform, and Customer owns all right, title, and interest in the Customer Content. Except as expressly set forth in this Agreement, each party retains all right, title, and interest in and to its intellectual property rights. All rights not expressly granted are reserved, and no license, covenant, immunity, transfer, authorization, or other right will be implied, by reason of statute, estoppel, or otherwise, under this Agreement.

3. **Charges and Payment**. This Section 3 only applies when a Customer purchases subscriptions to the Figma Platform directly from Figma (and not via a Reseller).

3.1. **Fees**. Customer will pay Figma all fees described in an Order in accordance with the terms therein and the GSA Schedule Pricelist. Unless otherwise specified herein or in an Order, (a) all fees are stated and solely payable in U.S. Dollars, (b) payment obligations are non-cancelable and not subject to setoff, (c)fees paid are non-refundable and (d) quantities purchased cannot be decreased during the relevant Order Term. Customer is solely responsible for any bank fees, interest charges, finance charges, overdraft charges, and any other fees Customer incurs as a result of the charges billed by Figma. If the Order automatically renews, Figma may change the fees applicable to a renewal by providing Customer at least 45 days' written notice of the new fees before the end of the then-current Order Term For clarity, any change in fees will not apply to the then-current
Order Term.

3.2. **Payment**. Unless otherwise specified in an Order or this Section, Customer will be invoiced annually upfront, with full payment due 30 days from the date of the applicable invoice. If Customer purchases its subscription online, fees are due at the time of purchase. Unpaid amounts are subject to a finance charge of 1.5% per month on any outstanding balance, or the maximum permitted by law, whichever is lower. In the event that Customer fails to pay the full amount owed under an Order, Figma may limit Customer's access to the Figma Platform, in addition to any other rights or remedies Figma may have..

3.3. **Taxes**. Fees do not include taxes. Each party is responsible for the payment of all taxes (including any interest and penalties) in connection with this Agreement that are imposed on that party by law. For Customer, such taxes may include sales/use, gross receipts, value-added, GST, personal property, excise, consumption, and other similar taxes or duties. Each party will be responsible for its own income taxes, employment taxes, and real property taxes.

3.4. **Withholding**. All payments made by Customer to Figma under this Agreement will exclude any deduction or withholding. If any such deduction or withholding (including cross-border withholding taxes) is required by law, Customer will pay such additional amounts as are necessary so that the net amount received by Figma after such deduction or withholding will be equal to the full amount that Figma would have received if no deduction or withholding had been required. Each party will use commercially reasonable efforts to work with the other party to help obtain, reduce, or eliminate any necessary withholding, deduction, or royalty tax exemptions where applicable.

4. **Confidentiality**.

4.1. **Confidential Information**. Each party (the "**Discloser**") has disclosed or may disclose proprietary or non-public business, technical, financial, or other information in anticipation of this Agreement or during the term of this Agreement ("**Confidential Information**") to the other party (the "**Recipient**"). Confidential Information of Figma expressly includes non-public information regarding features, functionality, and performance of the Figma Platform, and Confidential Information of the Customer expressly includes Customer Content. However, Confidential Information excludes any information that: (a) is or becomes generally available to the public without action or omission by Recipient; (b) was in the Recipient's possession or known by it prior to receipt from the Discloser; (c) was rightfully disclosed to the Recipient without restriction by a third party; or (d) was independently developed by Recipient without use of or reference to any Confidential Information of the Discloser.

4.2. **Obligations**. The Recipient will use the Discloser's Confidential Information only to exercise its rights and fulfill its obligations under this Agreement, including, in Figma's case, to provide the Figma Platform to Customer. The Recipient will use reasonable care to protect against disclosure of the Discloser's Confidential Information to parties other than the Recipient's employees, contractors, Affiliates, agents, or professional advisors ("**Representatives**") who need to know it and who have a legal obligation to keep it confidential. The Recipient will ensure that its Representatives are subject to confidentiality obligations that are no less restrictive than those herein. Notwithstanding the foregoing, the Recipient may disclose the Discloser's Confidential Information: (a) if directed by Discloser; or (b) to the extent required by applicable legal process, provided that the Recipient uses commercially reasonable efforts to (i) promptly notify the Discloser in advance, to the extent permitted by law and (ii) comply with the Discloser's reasonable requests regarding its efforts to oppose the disclosure. With respect to each Order, the obligations set forth herein will survive for the duration of the Order Term and five years following the expiration or termination of such Order.

5. **Warranties**.

5.1. **Mutual Warranties**. Each party represents and warrants to the other that: (a) this Agreement has been duly executed and delivered and constitutes a valid and binding agreement enforceable against the executing party in accordance with its terms; (b) the execution, delivery, and performance of this Agreement by the executing party does not violate the terms or conditions of any other agreement to which it is a party or by which it is otherwise bound or require authorization or approval from any third party; and (c) it will perform its rights and obligations under this Agreement in accordance with applicable law.

5.2. **Figma Warranties**. Figma represents and warrants to Customer during the applicable Order Term that: (a) Figma will provide access to the Figma Platform and any applicable support services in substantive conformity with the Documentation; and (b) Figma will employ applicable industry standard measures to protect the Figma Platform, in the form provided to Customer by Figma, against software viruses, Trojan horses, worms, or other similar malicious programs or code.

5.3. **DISCLAIMER**. EXCEPT FOR THE EXPRESS REPRESENTATIONS AND WARRANTIES STATED IN THIS SECTION 5, THE PARTIES MAKE NO REPRESENTATION OR WARRANTY OF ANY KIND WHETHER EXPRESS, IMPLIED (EITHER IN FACT OR BY OPERATION OF LAW), OR STATUTORY, AS TO ANY MATTER WHATSOEVER RELATING TO THIS AGREEMENT. FIGMA EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUALITY, ACCURACY, TITLE, AND NON-INFRINGEMENT. NON-FIGMA RESOURCES ARE PROVIDED BY THIRD PARTIES, NOT FIGMA, AND ANY USE OF NON-FIGMA RESOURCES IS SOLELY BETWEEN CUSTOMER AND THE APPLICABLE THIRD PARTY PROVIDER. FIGMA DOES NOT WARRANT OR SUPPORT,

AND WILL NOT HAVE ANY RESPONSIBILITY OR LIABILITY OF ANY KIND FOR, NON-FIGMA RESOURCES.

6. **Indemnity**.

6.1. **Indemnification by Figma**.

(a) Figma will have the right to intervene to defend Customer from any third party claim, action, suit, or demand (a "**Claim**") based on an allegation that the Figma Platform violates, infringes, or misappropriates any third-party copyright, patent, trade secret, or trademark, and will indemnify Customer for any costs, liabilities, damages, or other amounts (including reasonable attorneys' fees) actually paid or payable to unaffiliated third parties ("**Losses**") resulting from such Claim.

(b) Figma will have no obligation to defend or indemnify Customer for any Claim under Section 6.1(a) to the extent it is based on: (i) Customer's failure to use updates or modifications to the Figma Platform that Figma makes available to Customer that would have helped avoid or mitigate the Claim had they been used; (ii) the combination, operation, or use of the Figma Platform with third-party equipment, devices, software, application, systems, or data, including Non-Figma Resources, where the infringement would not have occurred but for such combination, (iii) use of the Figma Platform by Customer or Customer's Authorized Users in violation of this Agreement, or (iv) Customer Content.

(c) If Customer's use of the Figma Platform is, or in Figma's reasonable discretion is likely to be, subject to a Claim that may give rise to a defense or indemnity obligation under Section 6.1(a), Figma may, at its sole discretion and at no charge to Customer (and in addition to Figma's obligations to Customer under Section 6.1(a)): (i) procure for Customer the right to continue using the Figma Platform in accordance with this Agreement; (ii) replace or modify the Figma Platform so that it is non-infringing and includes substantially similar functionality as the original Figma Platform; or (iii) if options (i) and (ii) above are not commercially practicable in Figma's reasonable discretion, Figma may terminate Customer's right to use the impacted portion of the Figma Platform (in which case, Customer will immediately stop using the impacted portion of the Figma Platform) and provide a pro-rata refund of any pre-paid fees for the impacted service that remain unused as of the date of termination.

(d) THIS SECTION 6.1 SETS FORTH FIGMA'S SOLE AND EXCLUSIVE OBLIGATIONS, AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES, WITH RESPECT TO ANY ACTUAL OR ALLEGED INFRINGEMENT OR MISAPPROPRIATION OF ANY THIRD PARTY INTELLECTUAL PROPERTY RIGHT BY THE FIGMA PLATFORM AND ANY OTHER TYPE OF CLAIM SPECIFICALLY COVERED UNDER FIGMA'S INDEMNITY OBLIGATION (IF ANY). NO PARTY TO THIS AGREEMENT WILL BE ENTITLED TO ANY FORM OF IMPLIED OR EQUITABLE INDEMNIFICATION AT ANY TIME, WHETHER BASED ON A THEORY OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, WARRANTY, OR ANY OTHER THEORY OF LIABILITY, AND ANY RIGHT THERETO IS HEREBY IRREVOCABLY WAIVED AND DISCLAIMED BY EACH OF THE PARTIES.

6.2. Customer will defend Figma from any Claim based on Customer Content or use of the Figma Platform by Customer (or Customer's Authorized Users) in violation of this Agreement, and Customer will indemnify Figma from any Losses resulting from any such Claim.**Process**. If a party entitled to indemnification (the "**Indemnified Party**") becomes aware of any indemnifiable Claim, such party will give the other party (the "**Indemnifying Party**") written notice of the Claim as soon as reasonably practicable. The Indemnified Party will cooperate, at the expense of the Indemnifying Party, with the Indemnifying Party and its counsel in the defense or settlement of the Claim, and will allow the Indemnifying Party to have sole control of the defense or settlement. Subject to the prior sentence, the Indemnified Party will have the right to participate fully, at its own expense, in the defense of such Claim. To take advantage of the indemnity, the Indemnified Party must use all commercially reasonable efforts to mitigate its Losses. The Indemnified Party is not required to admit liability, except as required by applicable law, and any compromise or settlement of a Claim requiring the Indemnified Party to admit liability or to pay any money will require the prior written consent of both parties, such consent not to be unreasonably withheld or delayed. The indemnity obligations of the Indemnifying Party will be contingent on the Indemnified Party's compliance with this process.

7. **Limitations of Liability**.

7.1. **Limitation on Indirect Liability**. EXCEPT FOR EXCLUDED CLAIMS, UNDER NO CIRCUMSTANCES, AND UNDER NO LEGAL THEORY (WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, WARRANTY, OR ANY OTHER THEORY OF LIABILITY), WILL EITHER PARTY, ITS AFFILIATES AND ITS OR THEIR CONTRACTORS, EMPLOYEES, AGENTS, OR THIRD-PARTY PARTNERS, LICENSORS, OR SUPPLIERS (COLLECTIVELY, ITS "**PARTY REPRESENTATIVES**"), BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES (INCLUDING LOSS OF PROFITS, DATA, OR USE OR COST OF COVER) ARISING OUT OF OR RELATING TO THIS AGREEMENT OR THE USE OF OR THE INABILITY TO USE THE FIGMA PLATFORM, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7.2. **Limitation on Amount of Liability**. EXCEPT FOR EXCLUDED CLAIMS, UNDER NO CIRCUMSTANCES, AND UNDER NO LEGAL THEORY (WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, WARRANTY, OR ANY OTHER THEORY OF LIABILITY), WILL THE TOTAL LIABILITY OF EITHER PARTY, ITS AFFILIATES, AND ITS OR THEIR PARTY REPRESENTATIVES FOR ANY AND ALL DAMAGES AND CAUSES OF ACTION ARISING OUT OF OR RELATING TO THIS AGREEMENT OR THE USE OF OR THE INABILITY TO USE THE FIGMA PLATFORM, EXCEED, IN THE MAXIMUM AGGREGATE, THE FEES PAID AND PAYABLE TO FIGMA UNDER THE CUSTOMER'S APPLICABLE ORDER IN THE TWELVE-MONTH PERIOD PRIOR TO THE DATE ON WHICH THE DAMAGE OCCURRED.

7.3. **IN GENERAL**. EACH PROVISION OF THIS AGREEMENT THAT PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF WARRANTIES, OR EXCLUSION OF DAMAGES IS TO ALLOCATE THE RISKS OF THIS AGREEMENT BETWEEN THE

PARTIES. THIS ALLOCATION IS REFLECTED IN THE PRICING OFFERED BY FIGMA TO CUSTOMER AND IS AN ESSENTIAL ELEMENT OF THE BASIS OF THE BARGAIN BETWEEN THE PARTIES. EACH OF THESE PROVISIONS IS SEVERABLE AND INDEPENDENT OF ALL OTHER PROVISIONS OF THIS AGREEMENT. THE LIMITATIONS IN THIS SECTION 7 WILL APPLY TO THE MAXIMUM EXTENT NOT PROHIBITED BY LAW AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY IN THIS AGREEMENT.

8. **Term and Termination**.

8.1. **Term**. The term of this Agreement will commence on the Subscription Start Date of the first Order entered into between the parties and will continue until all Orders hereunder expire or until terminated in accordance with this Section 8, whichever happens first.

8.2 **Termination**. Either party may terminate an individual Order or this Agreement upon written notice to the other party, if the other party materially breaches this Agreement and such breach is incapable of cure, or with respect to a breach capable of cure, the breaching party does not cure such breach within 30 days of receiving notice of it. Either party may terminate or suspend an individual Order or this Agreement upon written notice to the other party without a cure period if (a) the other party breaches any of the terms relating to such party's intellectual property rights or Confidential Information, or (b) if the other party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation, or assignment for the benefit of creditors.

8.3. **Effect of Termination**. Termination of this Agreement will result in termination of all ongoing Orders; however, termination of a single Order will not result in termination of this Agreement or any other ongoing Orders. If Customer terminates under Section 8.2, Figma will provide Customer a pro rata refund of prepaid unused fees applicable to the remainder of the Order Term for any terminated Order. If this Agreement or any Order is terminated for any other reason, Customer will not receive a refund and will pay all fees as if the Order had not been terminated. Upon any termination, to the extent permitted by applicable law, Figma will make all Customer Content then held by Figma pursuant to the applicable Order available to Customer for electronic retrieval for a period of 30 days, but thereafter Figma will delete or retain any stored Customer Content as directed by Customer. The following sections of this Agreement will survive any expiration or termination of this Agreement: 2, 4, 5.3, and 7-9.

9. **Miscellaneous**.

9.1. **Affiliates**. A Customer Affiliate may enter into an Order under this Agreement and, in such case, by entering into the Order, the Affiliate agrees to be bound by the terms and conditions of this Agreement with respect to such Order and such Affiliate will be considered to be Customer, as such term is used herein, with respect to such Order. This Agreement is intended for the benefit of the parties who have entered into an Order under this Agreement and their respective permitted successors and assigns, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

9.2. **Product-Specific Terms.** Certain Figma offerings are subject to Product-Specific Terms (such as optional beta features, free trials, and Figma APIs) attached hereto. If Customer elects to use such offerings, the applicable Product-Specific Terms apply.

9.3. **Force Majeure**. In accordance with FAR Clause 52.212-4(f), Neither party will have any liability for failures or delays resulting from that party experiencing a Force Majeure Event. If a party experiences a Force Majeure Event, such party will: (a) promptly notify the other party of occurrence of the Force Majeure Event; and (b) use reasonable efforts to limit damages to the other party and to resume its performance under this Agreement. If a Force Majeure Event causes a party to fail to comply with its obligations under this Agreement for 30 or more consecutive days, either party may terminate this Agreement upon written notice, without liability. "**Force Majeure Event**" means any event or circumstance (other than a party's inability to satisfy payment obligations) that is outside a party's reasonable control, whether or not foreseeable.

9.4. **Notices**. All notices, requests, consents, claims, demands, waivers, and other communications under this Agreement (each, a "**Notice**") must be in writing (electronic mail sufficient) and sent to:

Figma: Contact identified in the Order

With a copy to: legal-notices@figma.com

Customer: Contact identified in the Order

9.5. **Severability; No Waiver**. The invalidity or unenforceability of any provision of this Agreement will not affect the validity or enforceability of any other provision hereof and it is the intent and agreement of the parties that this Agreement will be deemed amended by modifying such provision to the extent necessary to render it valid, legal, and enforceable while preserving its intent or, if such modification is not possible, by substituting another provision that is legal and enforceable and achieves the same objective. No failure or delay by either party in exercising any right under this Agreement will constitute a waiver of that right.

9.6. **Assignment**. This Agreement is not assignable or transferable by either party without the other party's prior written consent, except that either party may (without the other party's prior written consent) assign this Agreement, in whole, in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of such party's assets, . Any purported assignment in violation of this section is null and void.

9.7. **Service Providers**. For the avoidance of doubt, Figma may engage third party service providers to support its performance of this Agreement (including the subprocessors listed at https://www.figma.com/sub-processors/). Nevertheless, Figma will remain responsible for compliance with this Agreement.

9.8. **No Partnership**. No agency, partnership, joint venture, or employment is created as a result of this Agreement, and neither party has any authority of any kind to bind the other party.

9.9. **Governing Law and Dispute Resolution**. This Agreement shall be governed by the Federal laws of the United States.

The United Nations Convention on Contracts for the International Sale of Goods is specifically disclaimed.

9.10. **Export Control**. The Figma Platform and Customer's use thereof is subject to export control and economic sanctions laws and regulations (collectively, "**Export Controls**"), including the U.S. Export Administration Regulations, the laws, statutes, regulations, rules, and executive orders administered by the Office of Foreign Assets Control of the U.S. Department of the Treasury ("**OFAC**"). Figma and Customer each represents that it is not on (or owned or controlled by any person identified on) the OFAC Specially Designated Nationals and Blocked Persons List or any other list of prohibited or restricted parties promulgated under Export Controls. Customer must comply with all applicable Export Controls in its access to and use of the Figma Platform and Customer Content. Customer will not access or use the Figma Platform, export, re-export, distribute, assign, or otherwise engage in any transaction relating to the Figma Platform or any Customer Content in violation of Export Controls. For the avoidance of doubt, Figma may take measures required by law or governmental authority to comply with its obligations under Export Controls and OFAC (such as suspending access to the Figma Platform, terminating this Agreement, or blocking the relevant Customer Content).

9.11. **Anti-Corruption**. Neither party has received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from an employee or agent of the other party in connection with this Agreement. Reasonable gifts and entertainment provided in the ordinary course of business do not violate the above restriction.

9.12. **Government Use**. This Section 9.12 only applies if Customer is a government or public sector entity. Customer represents and warrants to Figma that it is entering into this Agreement in compliance with any applicable public procurement laws and regulations. If Customer is a U.S. government or U.S. public sector entity (or use of the Figma Platform is for the U.S. government), the Figma Platform and Documentation are "commercial products" (as defined at 48 C.F.R. §2.101), consisting of "commercial computer software" and "commercial computer software documentation" (as used in 48 C.F.R. §12.212 and 48 C.F.R. §227.7202, as applicable). In accordance with 48 C.F.R. §12.212 and 48 C.F.R. §227.7202-1, as applicable, the rights of the U.S. Government to use, modify, reproduce, release, perform, display, or disclose commercial computer software and commercial computer software documentation associated with the Figma Platform will be as provided in this Agreement. If a U.S. Government agency or end user has a need for rights not conveyed under these terms, it must negotiate with Figma to determine if there are acceptable terms for transferring such rights, and a mutually acceptable addendum to

this Agreement will be required in any applicable contract or agreement. The sections in this Agreement titled "Governing Law and Dispute Resolution," "Indemnification by Customer," any auto-renewal terms, and any other terms inconsistent with applicable law are hereby waived to the extent necessary to conform to applicable law.

9.13. **Trademark Guidelines**. Figma's Trademark Guidelines apply to any use by Customer of words, logos, graphics, designs, and other indicators that identify Figma as the source of a product or service ("**Figma's Marks**"). If Customer uses Figma's Marks, Customer will comply with Figma's Trademark Guidelines available at https://www.figma.com/using-the-figma-brand/.

9.14. **Interpretation**. Whenever the words "including," "include," "includes," or "such as" are used herein, they will be deemed to be followed by the phrase "without limitation."

9.15. **Entire Agreement**. This Agreement supersedes all other agreements between the parties relating to its subject matter. In the event of any conflict among any Orders, any Product-Specific Terms, and the terms of this Figma Software Services Agreement, the order of precedence will be: (a) the Product-Specific Terms; (b) the terms of this Figma Software Services Agreement; and (c) the Orders (from newest to oldest) unless such Order expressly overrides the foregoing terms. The parties agree that any terms and conditions stated in a Customer purchase order or other Customer ordering documentation (including any vendor management portal) are void.

Exhibit A – Definitions

1. **Defined Terms**. The following capitalized terms will have the meanings set forth below:

1.1. "**Affiliate**" means, with respect to any entity, any other entity that, directly or indirectly through one or more intermediaries, controls, is controlled by, or under common control with such entity. As used in this definition, "control" (including, with correlative meanings, "controlled by" or "under common control with") means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of such entity, whether through ownership of voting securities, by contract or otherwise.

1.2. "**Agreement**" means this Software Services Agreement (together with its exhibits and addenda), and any Product-Specific Terms.

1.3. "**Authorized Users**" means employees, contractors, and other persons associated with the Customer or its Affiliates who access or use the Figma Platform through the Customer's account.

1.4. "**Customer Content**" means applications and materials that are developed by Customer or its Authorized Users on the Figma Platform or uploaded to the Figma Platform by Customer or its Authorized Users.

1.5. "**Documentation**" means Figma-provided documentation available at https://help.figma.com/hc/en-us or such successor link identified by Figma.

1.6. "**Excluded Claims**" means damages resulting from (1) either party's willful misconduct, fraud, or gross negligence (including gross negligence or willful misconduct that results in personal injury or death), or (2) infringement by a party of the other party's intellectual property rights.

1.7. "**Figma**" means Figma, Inc.

1.8. "**Figma Platform**" means the Figma offerings identified in an Order, including any related mobile and desktop applications, early access features, integrations and resources developed by Figma for use with the Figma offerings identified in an Order, and Documentation. For the avoidance of doubt, the "Figma Platform" excludes Non-Figma Resources.

1.9. "**Non-Figma Resources**" means applications and materials that are developed or otherwise provided by a party other than Figma, including design files, plugins, component libraries, services, products, platforms, integrations, and code components.

1.10. "**Order**" means (a)(i) an ordering document or online order that is entered into between Figma and Customer or (ii) an ordering document that is entered into between Reseller and Figma, and (b) specifies, among other things, the Figma offerings purchased by, or on behalf of, Customer.

1.11. "**Order Term**" means the subscription term length set forth in the applicable Order or, with respect to early access features, the evaluation period set forth by Figma.

1.12. "**Product-Specific Terms**" means the terms and conditions attached hereto and available at www.figma.com/product-specific-terms/, which apply to certain Figma offerings.

1.13. "**Reseller**" means a third party authorized by Figma to resell the Figma Platform.

1.14. "**Territory**" means worldwide with the exception of: (1) jurisdictions that are embargoed or designated as supporting terrorist activities by the United States Government; and (2) jurisdictions whose laws do not permit engaging in business with Figma or use of the Figma Platform.

Exhibit B – Figma Security Standards

1. **Definitions**. For purposes of this **Exhibit B**, the following terms apply:

1.1. **"Authorized Affiliate"** means any of Customer's Affiliate(s) which: (i) (a) is subject to the Data Protection Laws; and (b) is permitted to use the Figma Platform pursuant to the Agreement between Customer and Figma but has not signed its own Order Form with Figma and is not a "Customer" as defined under the Agreement; and (ii) if and to the extent Figma processes Personal Data for which such Affiliate(s) qualify as the Controller (as defined under applicable Data Protection Laws).

1.2. "**Customer Data**" means Customer Content and Customer Personal Data.

1.3. "**Customer Personal Data**" means Personal Data pertaining to Customer's logged-in Authorized Users of the Figma Platform Processed by Figma on behalf of Customer (or an Authorized Affiliate) under this Agreement.

1.4. "**Data Protection Laws**" means all data privacy, data protection, and cybersecurity laws, rules and regulations of the United States, the European Union, and the United Kingdom, and similar national laws of Switzerland, to which the Customer Personal Data are subject. "Data Protection Laws" will include the California Consumer Privacy Act of 2018 ("**CCPA**"), the California Privacy Rights Act ("**CPRA**"), the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, the Virginia Consumer Data Protection Act, and the EU General Data Protection Regulation 2016/679 ("**GDPR**"), the UK Data Protection Act 2018 ("**UK GDPR**"), the Singapore Personal Data Protection Act of 2012 ("**PDPA**") and the Swiss Federal Act on Data Protection ("**Swiss FADP**"), that are applicable to the Processing of Personal Data under the Agreement.

1.5. "**Personal Data**" has the meaning assigned to the term "personal data" or "personal information" under applicable Data Protection Laws.

1.6. "**Process**" or "**Processing**" means any operation or set of operations which is performed on Customer Data or sets of Customer Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

1.7. "**Security Incident(s)**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data attributable to Figma.

1.8. "**Subprocessor**" means Figma's vendors and third party service providers that Process Customer Data.

1.9. "**Systems**" means the applications, databases, infrastructure, and platforms under Figma's control that are utilized to provide the Figma Platform to Customer.

2. **Policies and Codes of Conduct**

2.1. Figma maintains an Information Security Policy and reviews it at least annually, including after any major changes occur in applicable law or regulatory guidance or are otherwise made to the Systems.

2.2. Figma maintains codes of conduct and other policies covering anti-bribery and corruption, whistle-blowing, and other ethics policies (such as anti-money laundering and anti-slavery), and communicates these policies to all relevant staff. Figma's codes of conduct are available upon request.

2.3. Figma implements processes designed to ensure the ongoing compliance with these policies and to identify and enable Figma to take action against any areas of non-compliance. Failure to comply with policies are addressed through appropriate disciplinary actions.

3. **Information Security Program**

3.1. Figma assigns responsibility for information security management to senior personnel.

3.2. Figma implements technical and organizational measures designed to protect against unauthorized or unlawful processing of Customer Data and against accidental loss or destruction of, or damage to, Customer Data, including a written information security program, which includes policies, procedures, and technical and physical controls designed to ensure the security, availability, integrity, and confidentiality of Customer Data.

4. **Background Checks and Confidentiality**

4.1. Figma conducts pre-employment background screening on employees and contractors who will access Customer Data in the ordinary course of performing their job responsibilities, to the extent legally permissible and practicable in the applicable jurisdiction.

4.2. Figma requires all Figma employees and Subprocessors to execute a confidentiality agreement as a condition of employment or engagement and to follow policies on the protection of Customer Data.

5. **Access Control**

5.1. Figma assigns unique User IDs to authorized individual users to access Systems. All access to Systems must be authorized and authenticated.

5.2. Figma access rights to Customer Data are based on the principle of least privilege and designed to ensure that persons entitled to use a System have access only to the Customer Data for which they have a business need.

5.3. Figma maintains an accurate and up to date list of all personnel who have access to Systems and has a process to promptly disable within one business day of transfer or termination.

5.4. Figma periodically reviews and revokes Systems access rights, as needed, and logs and monitors such access.

5.5. Non-privileged users are prohibited from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards/countermeasures.

5.6. Figma maintains a password management policy designed to ensure strong passwords consistent with industry standard practices and requires the use of multi-factor authentication to access Systems. Passwords are promptly changed if Figma becomes aware that an account has been compromised.

5.7. Figma implements controls designed to ensure that Systems access is subject to appropriate authentication and user access controls:

- User IDs are unique and authorized;
- User accounts are granted the minimum required privileges to enable a user to perform their designated function;
- Access to audit trails is restricted and logged;
- Default accounts are deleted or disabled where possible and suitably authorized and controlled where this is not possible;
- Privileged accounts (e.g., administrator, root) are only used when technically required under change control procedures and not for day-to-day system operation;
- Where privileged account access is used, this access is logged and reviewed and access can be attributed to a named individual.

6. **Logging, Audit, and Accountability**

6.1. Figma creates, protects, and retains Systems audit records to maintain integrity and enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate Systems activity.

6.2. Figma reviews and analyzes Systems audit records on a regular basis to detect significant unauthorized activity with respect to Systems. Actions of Figma users can be uniquely traced to those users so they can be held accountable for their actions.

7. **System Change Control**

7.1. Figma establishes a configuration baseline for Systems using applicable information security standards, manufacturer recommendations, or industry standard practices. Monitoring is performed to validate that Systems are configured according to the established configuration baseline.

7.2. The introduction of new systems are controlled, documented, and enforced by the use of formal change control procedures including documentation, specifications, testing, quality control, recovery, and managed implementation.

7.3. Figma employs controls designed to secure source code, including version control, segregation of source code repositories, and least privilege access principles. Figma maintains separate and isolated environments for its development, testing, and production. Figma customer instances are logically separated.

7.4. Figma follows a structured secure development methodology, adheres to secure coding standards, and undergoes security assessment activities (e.g., dynamic and static scans) to identify and remediate security vulnerabilities before being released to production.

7.5. Figma employs reasonable controls designed to remove or disable unnecessary ports and services from Systems in accordance with the vendors' recommendations and settings.

8. **Vulnerability Management**

8.1. Figma maintains up-to-date anti-malware software, has implemented a vulnerability management program with regular scanning for vulnerabilities, subscribes to a vulnerability notification service, has a method for prioritizing vulnerability remediation based on risk, and has established remediation timeframes based on risk rating.

8.2. Once a patch is released, and the associated security vulnerability has been reviewed and assessed for its applicability and importance, the patch is applied and verified in a timeframe which is commensurate with the risk posed to Systems.

8.3. Penetration testing and vulnerability scanning is conducted on the Systems at least annually. Any remediation items identified as a result of the assessment are resolved as soon as possible on a timetable commensurate with the risk. Upon request, Figma will provide summary details of the penetration tests performed, findings, and whether the identified issues have been resolved.

8.4. Figma uses commercially reasonable efforts to regularly identify software vulnerabilities and, in the case of known software vulnerabilities, to provide relevant updates, upgrades, and bug fixes.

8.5. Figma deploys intrusion detection processes to monitor and respond to alerts which could indicate potential compromise of Customer Data.

8.6. Figma deploys a log management solution and retains logs produced by intrusion detection systems for a minimum period of one year.

9. **Capacity Planning**

9.1. Figma maintains a capacity management program that continuously and iteratively monitors, analyzes, and evaluates the performance and capacity of the Systems.

10. **Physical and Environmental Security**

10.1. Figma implements physical access control measures at Figma facilities and data centers designed to prevent unauthorized access to Systems (e.g., access ID cards, card readers, front desk officers, alarm systems, video surveillance, and exterior security).

11. **Security Incidents**

11.1. Figma maintains an information security incident management program that addresses management of Security Incidents.

11.2. Figma maintains an incident response plan that specifies actions to be taken in the event of a Security Incident.

11.3. Upon becoming aware of a Security Incident, Figma agrees to provide written notice without undue delay and within the time frame required under Data Protection Laws to Customer. A delay in giving such notice requested by law enforcement and/or in light of Figma's legitimate needs to investigate or remediate the matter before providing notice will not constitute an undue delay. Where possible, such notice will include all available details required under Data Protection Laws for Customer to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident. Figma's notification of or response to a Security Incident will not be construed as an acknowledgement by Figma of any fault or liability with respect to the Security Incident.

11.4. Figma will take reasonable measures to mitigate the risks of further Security Incidents.

12. **Subprocessors**

12.1. Figma will conduct a risk-based review of all Subprocessors designed to ensure that they implement appropriate technical and organizational measures.

12.2. Figma will enter into agreements with its Subprocessors that require such Subprocessors to secure and protect Customer Data by using at least the same degree of care outlined in this Exhibit B.

13. **Data Encryption**

13.1. Figma encrypts Customer Data in Figma's possession or control so that it cannot be read, copied, changed, or deleted by unauthorized personnel while in transit and storage, including when saved on removable media.

13.2. Keys are protected from unauthorized use, disclosure, alteration, and destruction, and have a backup and recovery process.

13.3 If a private key is compromised, all associated certificates will be revoked.

14. **Data Retention**

14.1. At the expiry or termination of this Agreement, Figma will, at Customer's request, delete or return all Customer Data (excluding any back-up or archival copies which will be deleted in accordance with Figma's data retention schedule), except where Figma is required to retain copies under applicable laws, in which case Figma will isolate and protect that Customer Data from any further Processing except to the extent required by applicable laws.

15. **Secure Disposal**

15.1. Figma implements controls designed to ensure the secure disposal of Customer Data in accordance with applicable law taking into account available technology so that Customer Data cannot be read or reconstructed.

15.2. Media will be securely erased electronically before disposal by overwriting or degaussing, or physically destroyed prior to disposal or reassignment to another system. Media cleansing/wipe products and processes prior to disposal comply with NIST SP 800-88 standard, "Guidelines for Media Sanitization" (or its successor) or equivalent industry standards.

16. **Risk Assessments**

16.1. Figma maintains a risk assessment program that includes regular risk assessments and controls for risk identification, analysis, monitoring, reporting, and corrective action.

16.2. At least annually, Figma will perform risk assessments (either internally or with contracted, independent resources) to identify risks to Customer Data, risks to Figma's business assets (e.g., technical infrastructure), threats against those elements (both internal and external), the likelihood of those threats occurring, and the impact upon the organization.

17. **Asset Management**

17.1. Figma will have an asset management program that classifies and controls hardware and software assets throughout their life cycle.

18. **Business Continuity and Disaster Recovery**

18.1. Figma will use industry standard practices for redundancy, robustness, and scalability designed to maintain the availability of the Figma Platform.

18.2. Figma implements and maintains contingency plans to address emergencies or other occurrences (for example, fire, vandalism, system failure, and natural disaster) that could damage or destroy Systems or Customer Data, including a data backup plan and a disaster recovery plan with at least annual testing of such plans. Figma may not modify such plans to provide materially less protection to the Customer without the Customer's prior written consent, which may not be unreasonably conditioned or withheld.

18.3. Backups are taken and recovery is tested on a regular basis.

19. **Security and Privacy Training**

19.1. Figma conducts mandatory training for Figma employees and relevant contingent workers, at least annually, on business ethics, privacy, and information security awareness. These trainings are reviewed for relevance and updated as needed, annually.

19.2. Teams associated with development efforts impacting Customer Data, undergo specific training focused on well-defined and secured coding practices.

20. **Security Control Testing**

20.1. At least annually, Figma will engage a qualified, independent external auditor to conduct periodic reviews of Figma's security practices against recognized audit standards, such as SOC 2 Type II and ISO 27001 certification audits (including surveillance and recertifications), as applicable. Upon request, Figma agrees to make such reports available to the Customer at compliance.figma.com (or a successor link identified by Figma).

21. **Data Protection Governance**

21.1. Figma assigns responsibility for data protection to senior personnel

Exhibit C – Addendum to Figma Software Services for Figma for Government (December 10, 2025)

This Figma for Government Addendum ("**Addendum**") entered into between Figma and Customer, and governs Customer's access to and use of Figma offerings provided under Figma for Government products. This Addendum is incorporated into and forms part of Customer's existing agreement with Figma for Figma Enterprise or Figma Organization (or if there is none, the Figma Software Services Agreement attached hereto and available at https://www.figma.com/ssa) ("**Agreement**"). Capitalized terms used but not otherwise defined in this Addendum shall have the meanings given to them in the Agreement.

This Addendum applies to Governmental Entities and Non-Governmental Entities purchasing Figma for Government products. To the extent the deviations set forth in this Addendum are required by applicable law, Figma and Customer agree that the following provisions take precedence over any conflicting terms in the Agreement:

1. Definitions.

1.1 "**Governmental Entities**" means state, local or federal departments or any independent establishments within the meaning of 5 U.S.C. § 101, 102, and 104(1), respectively, and any wholly owned Government corporation within the meaning of 31 U.S.C. § 9101.

1.2 "**Non-Governmental Entities**" means Customers purchasing Figma for Government products that are not Governmental Entities.

2. Terms applicable to both Governmental Entities and Non-Governmental Entities.

2.1 **FedRAMP Disclaimer**. In compliance with Figma for Government's current FedRAMP Moderate authorization, Customer will not, will ensure its Authorized Users do not (i) include Controlled Unclassified Information, Covered Defense Information, personal data, cardholder data or business sensitive information in support inquiries; or (ii) publish to the Figma Platform, or use the Figma Platform to distribute or create: any information that requires specific handling requirements and/or additional or tailored security controls beyond those provided by the Federal Risk and Authorization Management Program (FedRAMP) authorization level of the Figma Platform, including Classified or Controlled Unclassified Information.

2.2 **FedRAMP Status**. Figma will take commercially reasonable measures to maintain such FedRAMP or Impact Level status during the Order Term.

2.3 **Freedom of Information Act**. Figma recognizes that Federal agencies and information submitted to Federal agencies by prime contractors are subject to the Freedom of Information Act, 5 U.S.C. 552. To avoid any confusion, Confidential Information provided to Customer is provided within the meaning of Exemption 4, as it is both customarily and actually treated as private by Figma and provided to Customer under an assurance of privacy.

2.4 **Fees and Taxes**. The Fees do not include taxes and fees, including, but not limited to, any sales/use, gross receipts, value-added, personal property, excise, consumption, industrial funding fee, or contract access or similar fees. If the Customer provides appropriate evidence to establish

an exemption from any Federal, State, or local tax or duty, Figma will exempt the Customer from the associated tax or duty.

2.5 **Commercial Computer Software**. Figma for Government products were developed solely at private expense and are commercial computer software and related documentation within the meaning of the FAR and agency supplements thereto. In accordance with FAR 12.212 and DFARS 227.7202-1, as applicable, the rights of the Governmental Entity to use, modify, reproduce, release, perform, display, or disclose commercial computer software and commercial computer software documentation associated with the Figma for Government products will be as provided in the Agreement.

3. Terms applicable only to Governmental Entities

3.1 **Binding Agreement**. Pursuant to FAR 1.601(a) and 43.102, all provisions in the Agreement that would allow any individual, except for an authorized contracting officer or individually duly authorized by the contracting officer, to bind the Governmental Entity are deleted. The Governmental Entity warrants that individuals assigned as Administrative Users are duly authorized hereto.

3.2 **No Customer Indemnification Obligation**. If and to the extent applicable law prohibits a Governmental Entity from indemnifying Figma, any terms or conditions in the Agreement requiring the Governmental Entity to indemnify Figma shall be deemed void and not binding.

3.3 **Disputes**. For federal Governmental Entities, any dispute shall be subject to the Contract Disputes Act. For non-federal Governmental Entities, any dispute shall be subject to the process set forth in that Governmental Entity's applicable regulations.

3.4 **Termination**. As a commercial item contract, the termination rights for federal Governmental Entities are limited to those rights set forth in FAR 52.212-4. For non-federal Governmental Entities, any dispute shall be subject to the process set forth in that Governmental Entity's applicable regulations.

3.5 **Novation or Assignment**. Figma acknowledges that any assignment or novation will be subject to the Anti-Assignment Act and related regulations.

3.6 **Force Majeure**. Force Majeure delays shall be governed by FAR 52.212-4(f).

3.7 **Renewals**. Any clause that violates the Anti-Deficiency Act's ban on automatic renewal are hereby deemed to be deleted.

3.8 **Government Rights**. The Figma Platform is a commercial item, and any software therein is commercial computer software per FAR 12.211 and 12.212 and DFARS 227.7202, as applicable. Government Entities shall only have those rights in technical data, computer software, and computer software documentation (collectively, "data") set forth therein. This provision supersedes any FAR, DFARS, or other data rights clause or provision.

3.9 **Acceptance Criteria**. As commercial computer software, Figma for Government was not built to specific Governmental Entity requirements for purposes of acceptance. To the extent

acceptance is required by applicable law, Customer will have 5 business days ("**Acceptance Period**") after the Figma Platform is first made available to review and confirm the Figma Platform conforms with the Documentation. If Customer identifies a failure to conform to the Documentation, Customer must notify Figma within the Acceptance Period, in which case Figma will make reasonable efforts to address Customer's objection. If a resolution has not been agreed within five business days, Customer has five business days to terminate the applicable Order by written notice to Figma. Otherwise, the Figma Platform is deemed accepted under FAR 52.212-4(a).

3.10 **Liability**. To the extent the limitation of liability clause includes limitations on liability that are unenforceable under the FAR, DFARS, or other Federal or state procurement statute or regulation, that specific limitation is deemed to be deleted.

3.11 **Interest**. For the Federal ordering activity, fees not paid when due will accrue interest at a rate in accordance with the Prompt Payment Act or any other applicable Federal law.

3.12 **Indemnification.** 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.

Data Processing Addendum

Last updated: March 30, 2026

This Data Protection Addendum ("**Addendum**") forms part of the agreement(s) between Customer and Figma covering Customer's use of the Figma Platform to which this Addendum is incorporated ("**Agreement**") and governs Figma's processing of Personal Data in Customer Content.

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

1. Processing of Personal Data.

1.1. Description of Processing Activities. Details about processing activities, such as categories of data subjects and Personal Data processed are found in **Schedule 1** (Description of Processing).

1.2. Figma's Role. As a Processor, Figma will process Personal Data contained in Customer Content (including Personal Data of Customer's logged-in Authorized Users) only: (i) in accordance with documented Customer Instructions, or (ii) to comply with Figma's obligations under applicable laws and regulations.

1.3. Compliance with Law. Figma and Customer will each comply with Data Protection Law. Customer is responsible for ensuring Customer Instructions comply with Data Protection Law. Figma will notify Customer if it determines that an instruction infringes Data Protection Law.

1.4. Confidentiality. Figma must ensure that persons authorized to process Customer Content are subject to written or statutory obligations of confidentiality.

2. Security and Security Incidents.

2.1. Security Measures. Figma has implemented and will maintain appropriate technical and organizational measures designed to protect the security, confidentiality, integrity, and availability of Customer Content.

2.2 Security Incidents. Figma must notify Customer without undue delay and, where feasible, within 72 hours after becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Content processed by Figma and/or its Sub-processors ("**Security Incident**"). Figma will use commercially reasonable efforts to investigate and identify the root cause of

the Security Incident, and, to the extent within Figma's reasonable control, take reasonable and appropriate steps to mitigate and remediate the effects of the Security Incidents.

3. Sub-processors.

3.1 General Authorization. Customer generally authorizes Figma to engage third-party service providers to process Customer Content (each, a "**Sub-processor**"). Customer further agrees that Figma may engage its affiliates as Sub-processors.

3.2. Written Agreement. Figma will: (i) enter into written agreements with each Sub-processor that impose data protection obligations consistent with this Addendum; and (ii) remain liable to Customer where a Sub-processor fails to fulfill its data protection obligations.

3.3. Sub-processor List. Figma maintains an up-to-date list of Sub-processors, available at https://www.figma.com/sub-processors which contains details about Sub-processor functions, the location of processing, and a mechanism for Customers to subscribe to notification of new Sub-processors or replacement of existing Sub-processors.

3.4. Notification of Changes. At least fifteen (15) days before a new Sub-processor begins processing Customer Content, Figma will add the Sub-processor to its sub-processor list and, if Customer has subscribed to notifications, provide Customer with written notice ("**Sub-processor Notice Period**").

3.5. Objections to Sub-processors. Customers may object to Figma's appointment of a new Sub-processor during the Sub-processor Notice Period, provided such objection is in writing and based on reasonable grounds relating to data protection. In such an event, Figma and Customer agree to discuss commercially reasonable alternative solutions in good faith. If Figma and Customer cannot reach a resolution within the Sub-processor Notice Period, Figma may proceed with the appointment of the Sub-processor and Customer, as its sole and exclusive remedy, may terminate the applicable Order for the affected services by providing written notice to Figma.

4. Assistance and Cooperation.

4.1. Data Subject Rights. Taking into account the nature of the processing, Figma will provide reasonable and timely assistance to Customer to enable Customer to respond to requests from individuals exercising their rights, provided that Customer cannot reasonably fulfill such requests independently by using the self-service functionality of the Figm Platform**.**

4.2. Impact Assessments and Consultations. Taking into account the nature of the processing, Figma will provide reasonable assistance to Customer in connection with any

data protection impact assessment or consultation with any regulatory authority that may be required under Data Protection Law.

4.3. Government and Other Third-Party Requests for Customer Personal Data. If Figma receives a request from a third party, including a legally binding request from a governmental authority or law enforcement agency, for disclosure of Personal Data contained in Customer Content, Figma will (i) promptly notify Customer unless legally prohibited from doing so; (ii) where permitted, refer the requesting party to Customer; (iii) use reasonable efforts to challenge any request that is unlawful, disproportionate, or overbroad; and (iv) not disclose Personal Data contained in Customer Content unless required to do so by law.

5. Deletion and Return of Customer Personal Data. At the end of providing the Figma Platform to Customer, Figma will, as directed by Customer and at Customer's option, delete or return all Customer Content within thirty (30) days**.** Figma may retain Customer Content only to the extent required by Data Protection Law, subject to the confidentiality and processing restrictions in this Addendum.

6. Audit.

6.1. Audit Reports. Figma uses independent third-party auditors to verify the adequacy of its technical and organizational measures. Audits are performed at least once per calendar year at Figma's expense. Upon Customer's written request at reasonable intervals, and subject to appropriate confidentiality controls, Figma will make available information, including summaries of its then-current third-party certifications and audit reports, so Customer can verify Figma's compliance with its data protection obligations in this Addendum.

6.2. Audit Right. Only to the extent Customer's audit requirements under Data Protection Law cannot reasonably be satisfied through information provided in Section 6.1 (Audit Reports), Customer (or its appointed representative) may, at customer's expense, conduct an audit to assess Figma's compliance with this Addendum. Any audit must be: (i) subject to reasonable confidentiality controls; (ii) conducted during Figma's regular business hours; (iii) with 45 days' advance written notice; (iv) limited to once per year (unless required by a regulator or government authority); and (v) carried out in a manner that prevents unnecessary disruption to Figma's operations.

7. Region Specific Terms. Where Customer instructs Figma to process Customer Content originating in a region listed in **Schedule 2** (Region Specific Terms), the applicable regional terms will apply, including those governing international transfers of Customer Content.

8. Order of Precedence. If there is any conflict or inconsistency among the following documents, the order of precedence from highest to lowest will be: (1) the applicable terms stated in **Schedule 2** (Region Specific Terms), including any transfer provisions; (2) the main body of this Addendum; and (3) the Agreement.

9. Definitions. The following capitalized terms will have the meanings set forth below:

9.1. "Controller" (also referred to as "**Business**" under applicable Data Protection Law) means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

9.2. "Customer Content" means applications and materials that are developed by Customer or its Authorized Users on the Figma Platform or uploaded to the Figma Platform by Customer or its Authorized Users.

9.3. "**Customer Instructions**" mean: (i) processing to provide the Figma Platform and perform Figma's obligations in the Agreement (including this Addendum), (ii) investigating Security Incidents; and (iii) other reasonable documented instructions consistent with the terms of the Agreement. The parties agree that the Agreement and Customer's use of the features and functionality within the Figma Platform are Customer's complete and final instructions to Figma in relation to processing of Personal Data contained in Customer Content.

9.4. "**Data Protection Law**" means laws and regulations applicable to a party's respective processing of Personal Data under this Addendum.

9.5. "Figma Platform" means the Figma offerings, products and services.

9.6. "**Personal Data**" means information about an identified or identifiable natural person, or which otherwise constitutes "personal information," "personally identifiable information" or similar terms as defined in applicable Data Protection Law.

9.7. "**Processor**" (also referred to as "**Service Provider**" under applicable Data Protection Law) means the entity which processes Personal Data on behalf of the Controller.

Schedule 1 – Description of Processing

1. Categories of Data Subjects:

1.1. "**Authorized Users**" - employees, contractors, and other persons associated with the Customer or its Affiliates who access or use the Figma Platform through the Customer's account.

1.2. Other individuals whose Personal Data is included in Customer Content.

1.3. "**Visitors**" - visitors to Customer's publicly available Sites and Figma Make files.

2. Categories of Personal Data Processed:

2.1. Personal data contained in Customer Content, which includes:

2.1.1. Personal Data pertaining to Customer's logged-in Authorized Users (such as names and email addresses); and

2.1.2. Personal data of Visitors to Customer websites or pages created using the Figma Platform.

3. Sensitive Data or Special Categories of Data: Figma does not intend to receive or process sensitive or special categories of data.

4. The frequency of the transfer: Continuous.

5. Nature and Purpose of the Processing: Processing necessary to provide the Figma Platform in accordance with the Agreement.

6. Duration of the Processing: Prior to the termination of the Agreement, Figma will process Customer Content until Customer elects to delete such Customer Content via the self-service tools within the Figma Platform. Unless instructed to delete Customer Content, Figma will process Customer Content for the term of the Agreement and will then delete such data in accordance with Section 5 (Deletion and Return of Customer Personal Data) of the Addendum.

7. Onward Transfers to Sub-processors: Figma will transfer Customer Content to Sub-processors as permitted in Section 3 (Sub-processors).

Schedule 2 – Region Specific Terms

Unless otherwise defined in the Addendum or the Agreement, all capitalized terms used in this **Schedule 2** (Region Specific Terms) will have the meanings given to them in applicable Data Protection Law.

1. BRAZIL

1.1. "**Data Protection Law**" includes Lei Geral de Proteção de Dados Pessoais (LGPD).

1.2. The Brazilian Standard Contractual Clauses will apply to Personal Data in Customer Content that is transferred from Brazil, either directly or via onward transfer, to any country or recipient outside of Brazil that is not recognized by the Autoridade Nacional de Proteção de Dados (ANPD) as providing an adequate level of protection for Personal Data. For such

transfers, the Brazilian Standard Contractual Clauses are deemed entered into by Customer and Figma, incorporated into the Addendum by reference, and completed as follows:

(a) In Clause 1 of the Brazilian Standard Contractual Clauses, the identification of the parties are set forth in Annex I – List of Parties to this **Schedule 2** (Region Specific Terms).

(b) In Clause 2 of the Brazilian Standard Contractual Clauses, the description of the international data transfer is set forth in **Schedule 1** (Description of Processing) of the Addendum.

(c) In Clause 3 of the Brazilian Standard Contractual Clauses, OPTION B will apply, with onward transfers permitted in accordance with Section 3 (Sub-processors) of the Addendum. Figma Sub-processors can be found at https://www.figma.com/sub-processors.

(d) In Clause 4 of the Brazilian Standard Contractual Clauses, Customer remains responsible for compliance with Clause 14 (Transparency), Clause 15 (Data Subject Rights), and Clause 16 (Incident Reporting) of the Brazil Standard Contractual Clauses for any Personal Data of which it is the controller.

(e) In Section III of the Brazilian Standard Contractual Clauses, the security measures are set forth in Annex II – Technical and Organizational Measures to this **Schedule 2** (Region Specific Terms).

2. EUROPEAN ECONOMIC AREA

2.1. "**Data Protection Law**" includes the EU General Data Protection Regulation (GDPR) and (ii) the EU e-Privacy Directive.

2.2. The EU Standard Contractual Clauses ("**EU SCCs**") will apply to Personal Data in Customer Content that is transferred from the European Economic Area (EEA), including Iceland, Liechtenstein, and Norway, either directly or via onward transfer, to any country or recipient outside of the EEA that is not recognized by the relevant competent authority as providing an adequate level of protection for Personal Data. For such transfers, the EU SCCs are deemed entered into by Customer and Figma, incorporated into the Addendum by reference, and completed as follows:

(a) Modules

(i) Module Two (Controller to Processor) applies where Customer acts as a Controller and Figma acts as a Processor with respect to the Personal Data in Customer Content.

(ii) Module Three (Processor to Processor) applies where Customer acts as a Processor and Figma acts as a Sub-processor with respect to Personal Data in Customer Content.

(b) Clause-Specific Provisions

For each applicable Module:

(i) In Clause 7 of the EU SCCs, the optional docking clause does not apply.

(ii) In Clause 9 of the EU SCCs, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Section 3 (Sub-processors).

(iii) In Clause 11 of the EU SCCs, the optional language does not apply.

(iv) In Clause 17 of the EU SCCs, Option 1 applies, and the EU SCCs are governed by the law of Ireland.

(v) Clause 18(b) of the EU SCCs, disputes shall be resolved before the courts of Ireland.

(vi) In Annex I – Part A of the EU SCCs, the list of parties is set out in Annex I – List of Parties to this **Schedule 2** (Region Specific Terms).

(vii) In Annex I – Part B of the EU SCCs, the description of the transfer is set forth in **Schedule 1** (Description of Processing) of the Addendum.

(viii) In Annex I – Part C of the EU SCCs, the supervisory supervisory authority is the Irish Data Protection Commission.

(ix) In Annex II of the EU SCCs, the technical and organizational measures are set out in Annex II – Technical and Organizational Measures to this **Schedule 2** (Region Specific Terms).

(x) In Annex III of the EU SCCs, a list of Figma Sub-processors can be found at https://www.figma.com/sub-processors.

3. SWITZERLAND

3.1. "**Data Protection Law**" includes the revised Swiss Federal Act on Data Protection (FADP).

3.2. The EU SCCs will apply to Personal Data in Customer Content that is transferred from Switzerland either directly or via onward transfer, to any country or recipient outside of Switzerland that is not recognized by the relevant competent authority as providing an adequate level of protection for Personal Data. For such transfers, the EU SCCs are deemed entered into by Customer and Figma, incorporated into the Addendum by reference, and completed as follows:

(a) References in the EU SCCs to "Regulation (EU) 2016/679" will be interpreted as references to Swiss Data Protection Law, and references to specific Articles of that Regulation will be replaced with the equivalent sections of Swiss Data Protection Law.

(b) References to "EU", "Union", "Member State" or similar terms shall be interpreted to include Switzerland.

(c) In Clause 13 and Annex I(C) of the EU SCCs, the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner (FDPIC).\

(d) In Clause 17 of the EU SCCs, the laws of Switzerland are the governing law.

(e) In Clause 18(b) of the EU SCCs, disputes will be resolved before the courts of Switzerland.

(f) In Clause 18(c) of the EU SCCs, all references to Member State will be interpreted to include Switzerland and Data Subjects in Switzerland are not excluded from enforcing their rights in their place of habitual residence in accordance with Clause 18(c).

4. UNITED KINGDOM

4.1. "**Data Protection Law**" includes the UK Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).

4.2. The UK International Data Transfer Addendum to the EU SCCs ("**UK Addendum**") will apply to Personal Data that is transferred from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognized by the relevant United Kingdom authority as providing an adequate level of protection for Personal Data. For such transfers, the UK Addendum is deemed entered into by Customer and Figma, incorporated into this Addendum by reference, and completed as follows:

(a) In Table 1 of the UK Addendum, Customer's and Figma's details and key contact information are set forth in Annex I – List of Parties to this **Schedule 2** (Region Specific Terms).

(b) In Table 2 of the UK Addendum, the Approved EU SCCs, applicable Modules, and selected clauses are as described in Section 2 (European Economic Area) of this **Schedule 2** (Region Specific Terms)**.**

(c) In Table 3 of the UK Addendum:

(i) The list of parties is set forth in Annex I – List of Parties to this **Schedule 2** (Region Specific Terms).

(ii) The description of the transfer is set forth in **Schedule 1** (Description of Processing) of the Addendum.

(iii) The technical and organisational measures including technical and organisational measures to ensure the security of the data are set out in Annex II – Technical and Organizational Measures to this **Schedule 2** (Region Specific Terms).

(iv) The list of sub-processors is available at https://www.figma.com/sub-processors.

(d) In Table 4 of the UK Addendum, either party may terminate the UK Addendum in accordance with its terms.

5. UNITED STATES

5.1. Where Personal Data in Customer Content is subject to any applicable state privacy laws ("**U.S. State Privacy Laws**") and Figma acts as a Service Provider or Processor on behalf of Customer, Figma will process such Personal Data in compliance with applicable U.S. State Privacy Laws and only on Customer Instructions for the limited and specified purposes set out in the Addendum. Figma will not:

(a) retain, use, disclose, or otherwise process such Personal Data for any commercial purpose other than the limited and specified purposes contemplated by the Addendum, the Agreement, or as otherwise permitted under U.S. State Privacy Laws;

(b) "sell" or "share" such Personal Data within the meaning of applicable U.S. State Privacy Laws;

(c) retain, use, disclose, or otherwise process such Personal Data outside of the direct business relationship with Customer; or

(d) combine Personal Data with Personal Data obtained from other sources except as permitted by U.S. State Privacy Laws (e.g., to perform internal business operations, comply with law, or detect a Security Incident).

5.2. Figma will notify Customer if it determines that it can no longer meet its obligations under U.S. State Privacy Laws. Customer may take reasonable and appropriate steps to stop and remediate any unauthorized processing of Personal Data.

5.3. Figma certifies compliance with the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework program administered by the US Department of Commerce (collectively, the "**DP Framework**"). As required by the DP Framework, Figma (i) provides at least the same level of protection to Personal Data as is required by the DP Framework; (ii) will notify Customer if Figma makes a determination it can no longer meet its obligation to provide the

same level of protection as is required by the DP Framework principles, and (iii) will, upon written notice, take reasonable and appropriate steps to remediate any unauthorized Processing of Personal Data.

Annex I – List of Parties

A. LIST OF PARTIES

1. **Controller(s) / Data exporter(s)**:

Name: Customer.

Address: Customer address provided in the Agreement.

Contact person's name, position and contact details: As set out in the Agreement

Activities relevant to the data transferred: Processing of Customer Content for the purpose of the Agreement

Signature and date: See signature and date of the Addendum or, if the Addendum is incorporated in the Agreement by reference, see the signature (or electronic acceptance) and date of execution of the Agreement.

Role (controller/processor): Controller

2. Processor(s) / Data importer(s):

Name: Figma, Inc.

Address: As set out in the Agreement.

Contact person's name, position and contact details: As set out in the Agreement.

Activities relevant to the data transferred under these Clauses: Processing of Customer Personal Data for the purpose of the Agreement

Signature and date: See signature and date of the Addendum or, if the Addendum is incorporated in the Agreement by reference, see the signature (or electronic acceptance) and date of execution of the Agreement.

Role (controller/processor): Processor

Annex II – Technical and Organizational Measures

Technical and Organizational Security Measure	Evidence of the Technical and Organization Security Measure
Measures for confidentiality and encryption of Customer Personal Data	Encryption of Customer Personal Data at rest and in transit (TLS/SSL and AES-256 or equivalent) and other measures consistent with industry standards.
Measures for systems integrity and availability	Measures to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services, including robust backup and disaster recovery plans.
Measures for regular security testing and validation	Implementation of a comprehensive security program, including regular risk assessments, vulnerability scanning, and independent audits (e.g., SOC 2 Type 2, ISO 27001, and ISO 27018 certifications).
Measures for user access control and authentication	Policies and controls for user identification, authorization, and strong authentication mechanisms for accessing Customer Personal Data.
Measures for the physical security of data processing locations	Controls to ensure the physical security of data centers and facilities where Customer Personal Data is processed.
Measures for logging and monitoring	Logging of system events, security monitoring, and incident detection procedures.
Measures for limited data retention and deletion	Customer Personal Data is retained for the duration of the Agreement and deleted within 30 days post-termination, except where required by applicable Data Protection Law (as detailed in Section 5 (Deletion and Return of Customer Personal Data).
Measures for data portability and erasure	Customer can access, correct, return, or delete Customer Personal Data using the self-service functionality of the Figma Platform (as detailed in Section 5 (Deletion and Return of Customer Personal Data)).

Technical and Organizational Security Measure	Evidence of the Technical and Organization Security Measure
Measures for Sub-processor oversight	Written agreements with Sub-processors that impose data protection obligations no less protective than this Addendum (as detailed in Section 3 (Sub-processors)). The current list of Sub-processors is available at https://www.figma.com/sub-processors/

Acceptable Use Policy

Last Updated: March 26, 2026

This Acceptable Use Policy applies to your use of anything that Figma makes available, including Figma's SaaS platform, websites, and APIs (collectively, the "**Services**"). This policy outlines the standards of conduct we require on the Services and is designed to protect the integrity of the Services and other users. This policy may non-materially change as Figma grows and evolves, so please check back regularly for updates and changes.

1. Compliance with Laws and Regulations.

You are responsible for using the Service in compliance with all applicable laws and regulations and Figma's documentation or help pages.

2. Conduct Restrictions.

While using the Services, you may not:

a. damage, disable, override, interfere with, or circumvent any aspect of the Services (including any safety, integrity, or privacy filters, instructions, controls, safeguards, or other mechanisms offered by, as part of, or with the Services);

b. interfere with the Services operation (e.g., by exceeding or trying to exceed load specifications or by using the Services to generate synthetic data) or anyone else's use of the Services;

c. test, penetrate, or scan the Services for security vulnerabilities or limitations, other than in compliance with our bug bounty program;

d. impersonate anyone or misrepresent your connection with any person or entity;

e. use the Services to compete with Figma, or copy any ideas, features, functions, or graphics of the Services;

f. distribute any unwanted communication (e.g., using the Services to send spam);

g. use the Services for activities where use or failure of the Services could lead to death, bodily injury, damage to personal property, or environmental damage;

h. access or use the Services in a manner intended to avoid incurring fees owed (e.g. by repeatedly transferring a seat to and from the same user(s) to avoid paying for the appropriate number of seats needed, or by sharing account credentials – each user account is personal to the user to which it is issued);

i. act in bad faith;

j. scrape, data mine, or except as explicitly permitted by Figma, access Figma or Figma content (including third party content made available through Figma) programmatically;

k. use a third party's content without their permission (e.g., use stolen content);

l. deceive or mislead any person, including by indication, that any AI output was solely human generated or modify, tamper with, remove, obscure, or otherwise alter any metadata, digital signatures, or watermarks that identify AI output as generated using a generative artificial intelligence model;

m. use the Services in a way that causes, or is intended to cause, bias, harm, or discrimination against an individual or to make solely automated decisions about individuals which could have a legal or similarly significant effect;

n. modify, or use anything that modifies, Figma's code or code execution; or

o. use the Services in a manner that is intended to avoid applicable international sanctions with respect to an individual or organization.

3. Content Restrictions

You may not upload or publish to the Services, or use the Services to distribute, create, collect, or publish anything that:

a. is fraudulent, false, misleading, or deceptive;

b. is defamatory, obscene, pornographic, vulgar, or offensive;

c. promotes, or is intended to promote, discrimination, bigotry, racism, hatred, harassment, bullying, or harm against any individual or group;

d. is violent or threatening or promotes violence or actions that are threatening to any person or entity;

e. promotes illegal or harmful activities, goods, or substances, including but not limited to counterfeits, drug use, terrorism or human trafficking;

f. is malicious or destructive, such as software viruses, worms, trojan horses, spyware, dishonest adware, scareware, crimeware, or any other malicious or destructive software of programs;

g. is illegal or solicits conduct that is illegal under laws applicable to you or Figma;

h. violates the rights of others, including data privacy, confidentiality, and/or intellectual property rights (e.g., upload or publish stolen content);

i. is or includes sensitive information subject to regulation or protection under applicable laws, including but not limited to Special Category Data as defined under the General Data Protection Regulation (GDPR) (for example, data relating to race, religion, politics, health, genetics, biometrics, or sexual orientation);

j. is or includes patient, medical, or other personal health information (including but not limited to protected health information under HIPAA);

k. is or includes financial information, including but not limited to credit and debit card information;

l. is or includes social security numbers or other government identifiers (for example IDs or passports);

m. is or includes protected data about minors (such as data protected by the Children's Online Privacy Protection Act); or

n. is or includes any government related information that requires specific handling requirements and/or additional or tailored security controls beyond those provided by the Federal Risk and Authorization Management Program (FedRAMP) authorization level of the Figma Platform.

If you violate this policy or encourage, allow or assist others to do anything to violate this policy, we will take any action we consider necessary to protect Figma, our users, and third parties. This may include quarantining or deleting data stored on the Services, removing any of your content, or suspending your use or access to the Services. Please note that violation of this policy may result in termination in accordance with our termination rights in our agreement with you. You will not be entitled to any credit or other compensation for any interruption of the Services caused by your violation of this policy.

4. AI-Specific Considerations

If you choose to use Figma AI feature(s), you agree to comply with the following third party provider policies:

- OpenAI's Policies
- Jasper AI's Platform Guidelines, AUP, and Fair Use Policy
- AWS Responsible AI Policy
- Anthropic's Usage Policy
- Google's Generative AI Prohibited Use Policy and AUP

- Microsoft's AI Code of Conduct

If you choose to use images from Unsplash, you may not access, download, copy, modify, distribute, perform, or use those images to create or contribute to a service that is similar to or competitive with Unsplash.

Figma AI features may include filters, safety features, attribution requirements, or other restrictions that you are responsible for complying with. Please take care to review for these options/restrictions when using Figma AI features.

5. Copyright and IP

Figma respects copyright law and expects its users to do the same. Figma's Copyright and IP Policy.

Order Form Special Term

Figma Advisory Services - Strategic Success Plan. The fees set forth above for Figma Advisory Services - Strategic Success Plan are based on the initial quantity of seats purchased. The fees set forth above for Figma Advisory Services - Strategic Success Plan in this Order are fixed for the Order Term.

As part of the Figma Advisory Services - Strategic Success Plan, Customer has access to the following:

- **Dedicated Account Resources.** Dedicated Customer Engagement Manager ("CEM") and Technical Account Manager ("TAM"). These dedicated account resources will be based out of the United States.
- **Product Trainings.** Up to four introductory or advanced product trainings per three month period (e.g., "Intro to Figma Make"), prorated for periods less than 3 months.
- **Customized Solutions Services.** Up to five customized workflow services of five-hours each 12 month period (e.g., improving development efficiency, rapid prototyping for user testing), prorated for periods less than 12 months; provided Customer cannot exceed two customized workflow services during any 3 month period.
- **Technical Consultation Workshops.** Technical workshops (e.g., API guidance). Customer may select up to one customized workshop from Figma's workshop menu per three month period.
- **Engagement Channels.** A CEM-managed Slack or Microsoft Teams channel for ongoing communications.
- **Quarterly Success Reviews.** Quarterly business reviews including value assessments and ROI analyses.
- **Premium Support.** 24/7 email support and scheduled live Zoom consultations.

The benefits listed above are provided upon Customer request, must be used during the Order Term, and do not rollover. The Strategic Success Plan does not include delivery of any software, code, or other deliverables, and Figma cannot guarantee that the Strategic Success Plan will achieve any particular business outcome.

Governance+ for Figma

Figma will provide the Figma Governance+ offering described at https://help.figma.com/hc/en-us/articles/31825370509591-Governance-for-Figma, a current version of which is below.

Governance+ is available as an add-on for Figma Enterprise and Figma for Government. While most features are identical across both solutions, a small number differ—or are available on one plan only—due to the compliance requirements of the Figma for Government environment. See the table in What's included for a full comparison.

If your organization has unique security or compliance needs, Governance+ provides the specialized tools you need to manage your data, ensure safe access, and stay compliant.

With Governance+, you'll get:

- Centralized control: Make sure all Figma activity by your employees happens in the right instance and on your approved networks, where your policies apply. With features like IP Allowlist and Network Access Restrictions (NAR), you can minimize the risk of data slipping into unauthorized spaces or accounts.

- Account security: Protect your organization's data by enforcing secure authentication requirements. With Enforced Two-Factor Authentication (2FA), Extended Idle Session Timeout, and Multiple Identify Provider (IdP) support, you can reduce the risk that accounts with approved access to your organization's content are compromised.

- Data governance: Stay compliant with your organization's data standards. Governance+ gives you visibility into Figma activity through tools like the Discovery Pipeline, helping you meet electronic communication retention policies and support legal discovery requirements.

With Governance+, you can confidently scale Figma while meeting your organization's security and compliance standards. It's built to help you make Figma a compliant workspace where your team can focus on what matters most—creating together.

What’s included in Governance+?

Feature	Description	Figma Enterprise	Figma for Government
Restrict file exporting	Prevent view-only users from copying, saving, or exporting files	✓	✓
Network access restrictions (NAR)	Restrict unauthorized account access while on your network	✓	✓
IP allowlist	Ensure employees can only access their Figma account from the organization's network	✓	✓
Discovery pipeline	Log all text edits in Figma files to meet electronic communication retention requirements	✓	✓
Extended idle session timeout	Get more granular control over when inactive users are logged out	✓	— ‡
Enforced 2FA	Require additional authentication for members and guests	✓	✓
Multiple IdP support	Connect more than one identity provider and map domains to the right provider	✓	✓

Feature	Description	Figma Enterprise	Figma for Government
Internal policies	Require users to agree to customer-provided policies before accessing content	✓	✓
Enterprise Key Management (EKM)	Encrypt certain Figma file data at rest using your organization's AWS KMS key	✓	✓
Guest expiration	Set a default lifetime for newly invited guests and manage individual expiration dates	✓	✓
AI hosting controls	Manage where AI traffic is sent and where AI features can be used	✓	— ‡
Developer Logs API	Fetch a granular log of API calls made to the REST API or MCP server	✓	✓

The Governance+ feature details may vary between Figma Enterprise and Figma for Government. See the relevant section for details.

‡ Not part of Governance+ for Figma for Government. These features are already included in the Figma for Government baseline environment.

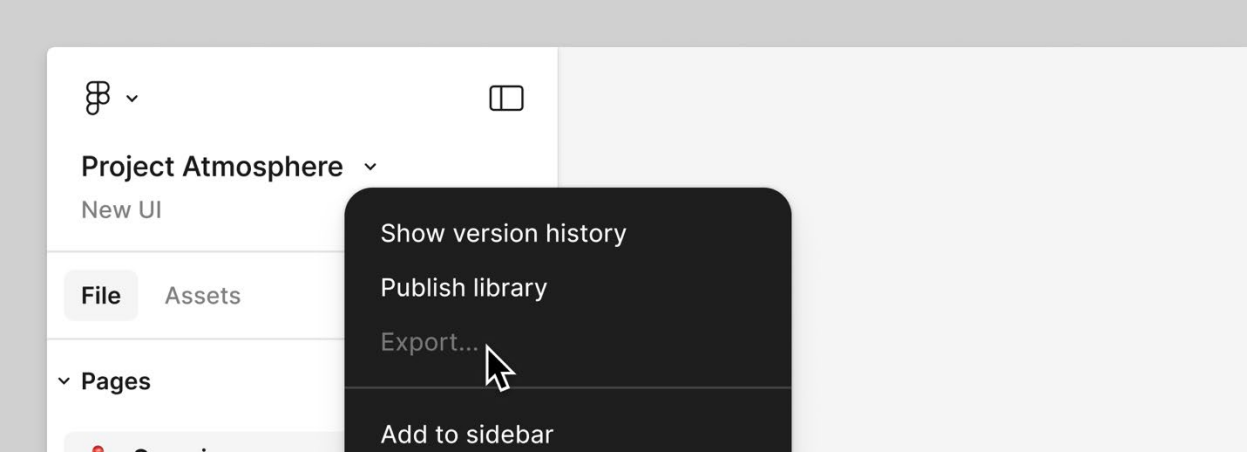
For pricing and packaging details, contact your sales representative.

Restrict file exporting

By default, anyone with view-only access to a file can export assets from it, save a local copy of it to their computer, or copy its contents from one file to another.

While users can restrict these actions on individual files, organization admins can enable the file export setting to create a consistent policy across the organization or selected workspaces.

When active, this setting restricts users with view-only access from copying, saving, or exporting files. Any actions related to saving, copying, or exporting are hidden or disabled for affected users.



The available options for this setting are:

- Allow exporting by all viewers. This is the default setting and allows all users to copy, save, and export from a file.
- Prevent exporting by guest viewers. Guests with view access aren't allowed to copy, save or export. Members of your organization with view-only or edit access—or guests with edit access—can still perform these actions.
- Prevent exporting for all viewers. Anyone with view-only access can't copy, save, and export. People with edit access to the file will still be able to perform these actions.

Note: Users can still disallow viewers from copying, saving, and exporting on a per-file basis—even if the organization has a more permissive file export setting enabled.
If your organization uses workspaces, an organization admin can apply the file export settings at the workspace level, not just the organization level. Workspace-level settings will take precedence over the organization-level settings.

Enable file export restrictions

1. From the file browser, click Admin.
2. Select the Settings tab.
3. Navigate to the External access section and click File exporting.

Network access restrictions

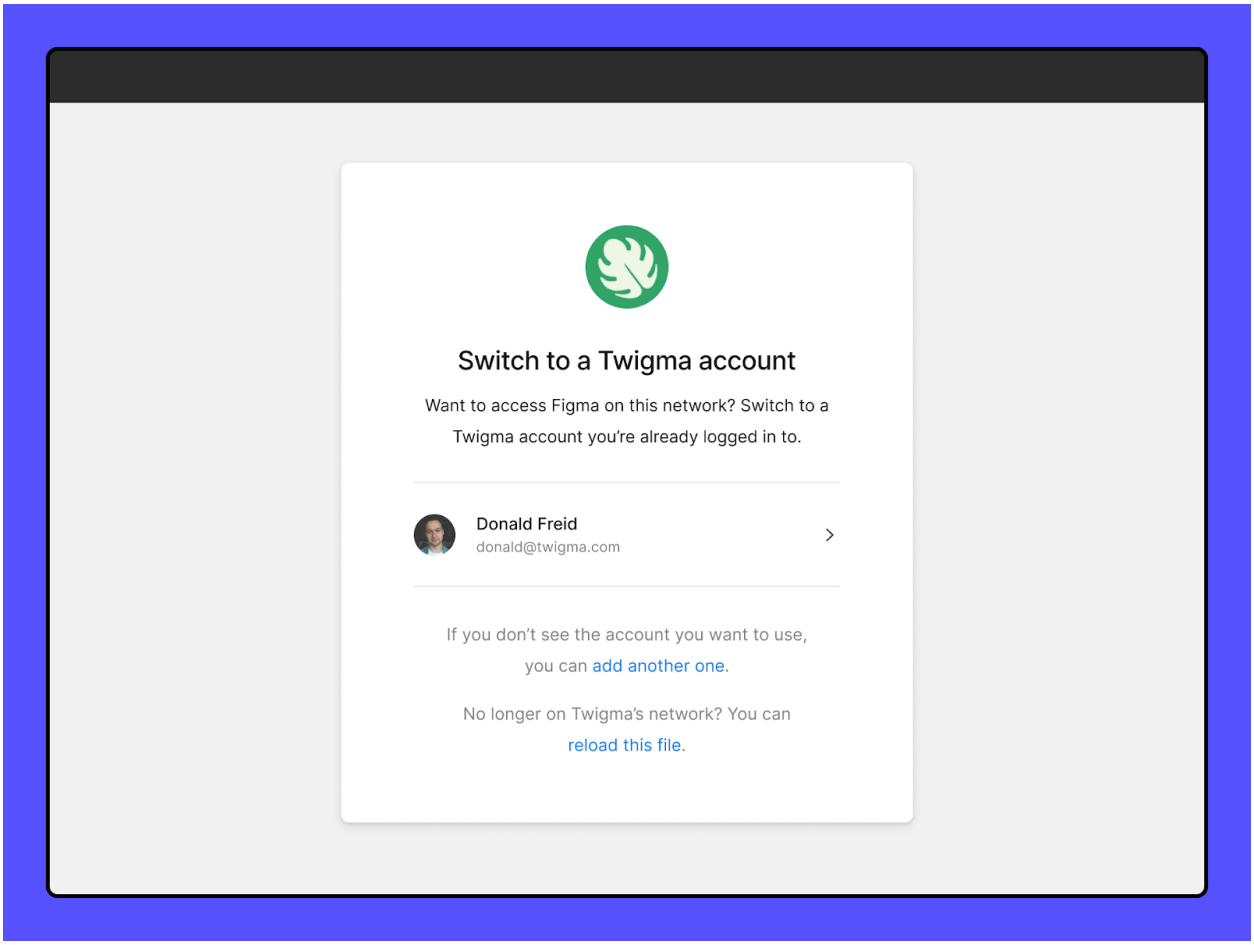
Organization admins can ensure secure collaboration by enabling the Restrict external account access on this network setting. This feature prevents users from accessing personal or unauthorized Figma accounts while connected to your corporate network.

Before NAR can be enabled, your organization must pass a shadow mode testing period. During this time, Figma monitors traffic at the provided IP ranges to verify that the majority of Figma users from those IP ranges are already members or guests in your organization's plan. NAR can only be enabled once this condition is confirmed.

Once enabled, users can only access Figma on the corporate network if:

- They log in with an account associated with your organization’s domain.
- They are guests in your organization.

Note: If an external user has a pending invite to join the organization, they won’t be able to accept the invitation while on the corporate network.
If someone tries to use an unauthorized Figma account while they're on the corporate network, they'll be prompted to switch to their work account:



When the person rejoins an external network, they can resume access to their other Figma accounts.

Enable or disable network access restrictions

To turn on this setting, provide the IP range(s) for your network and proof of ownership, such as a letter, email, or invoice from your ISP confirming the IP range assignment.

To get in touch with support:

- Figma Enterprise: Contact the support team via the support request form.
- Figma for Government: Email support-figgov@figma.com.

The process will take about two weeks to complete. You can find this setting by following the instructions below.

1. From the file browser, click Admin.
2. Select the Settings tab.

3. Navigate to External access and click Contact support.

IP allowlist

Note: All organization domains must be verified via technical domain verification (i.e., you must add a TXT record to your DNS records via your domain provider) before you can enable IP allowlist.
The IP allowlist ensures secure access to your organization's Figma account by limiting access to users connected to approved corporate networks. With this feature enabled, members of your organization can only authenticate and use their Figma accounts when they're within the specified IP ranges.

Once enabled, the IP allowlist enforces these rules:

- Applies to members only: Members are users with accounts on your organization's domain. Guests and organization admins are exempt.
- IP-based access checks: Figma examines all requests from members. If the request originates from an approved IP range, access is granted. Otherwise, members are prompted to switch networks or accounts. Only IPv4 addresses are supported.

Setting up the IP allowlist

To enable the IP allowlist for your organization:

1. Verify your domains via technical domain verification.
2. Add allowed IP ranges in the admin console:
    - Go to Admin → Settings → Login and provisioning → IP allowlist.
3. Keep IP ranges updated. If your corporate network changes, update the IP ranges in the admin console.

Discovery pipeline

The Discovery API helps meet compliance requirements by letting organizations extract all edits to text persisted in Figma files on a go-forward basis.

- Logs events whenever users edit text in comments, shapes, stickies, text boxes, component documentation, Dev Mode links, and more. Also captures the user-authored portion of prompts to AI features.

- Data is made available to customers via secure, short-lived downloadable files that are accessed by hitting a url that's returned via an API endpoint.

In Governance+ for Figma for Government, only the user-authored portion of Make prompts is captured (Figma Make is currently the only AI feature in Figma for Government). The Discovery API is accessed at https://api.figma-gov.com instead of https://api.figma.com.
Discovery pipeline data is only retained and available for querying for 30 days. To meet your data retention requirements, you should regularly query the endpoint and download the files from the provided links.

For setup and implementation, refer to the Discovery API developer documentation.

- Figma Enterprise: developers.figma.com
- Figma for Government: developers.figma-gov.com

Note: The discovery pipeline feature and API are not enabled by default with Governance+. To activate this feature, you must contact Figma Support.

Extended idle session timeout

This Governance+ feature is additive for Figma Enterprise only. Figma for Government includes idle session timeout as part of its baseline environment.
By default, Figma automatically logs users out after 21 days of inactivity. For added security, organization admins can configure an idle session timeout to log out inactive users earlier. With Governance+, timeouts can be set as short as 15 minutes.

How it works

- Idle session timeouts apply only to organization members, not guests.
- When a session times out, users are logged out across all platforms, including web browsers, desktop apps, mobile apps, embeds, and integrations (e.g., Microsoft Teams).
- Users receive a prompt to stay logged in when they are less than one minute away from timing out. If they don't respond, they must log back in to regain access.
- If a user belongs to multiple organizations with session timeouts, the shortest timeout applies.

Note: Figma's activity log captures changes to the session timeout policy and logs when members are logged out due to a timeout. Timeouts are logged immediately for open web browsers or desktop apps; background timeouts are logged the next time the user accesses Figma.

Set an idle session timeout

1. From the file browser, click Admin.
2. Select the Settings tab.
3. Under Login and provisioning, click Session timeout.
4. Click Custom timeout.
5. Choose a timeout length and click Save.

Note: Setting a new timeout resets inactivity for all users in your organization. Users will only be logged out after exceeding the newly defined timeout period.
If anyone in your organization cannot log back in after a timeout, please ask them to contact support.

Enforced 2FA

With Enforced 2FA, Enterprise organizations can restrict access to their content for guests who do not have two-factor authentication enabled. This feature enhances security by ensuring only properly authenticated users can access content.

2FA settings are available for both members and guests.

To help manage guest access, the admin console now includes:

- CSV Export: The members table CSV export now has a 2FA_enabled column, indicating whether guests who use username/password have 2FA enabled.
- Blocked Badge: Guests without 2FA will display a Blocked badge next to their name once 2FA is enabled.

Enforced 2FA for members

Who is impacted:

- Figma Enterprise: Applies only to members who authenticate using username and password. Members using SAML SSO or Google Login are excluded, but may set up 2FA directly with their identity provider.

- Figma for Government: Applies only to members who authenticate with magic links

Your organization's admins can configure this feature through the administration portal in your Figma account. It is a self-service feature.

1. From the file browser, select Admin in the sidebar.
2. Click the Settings tab.
3. In the Login and provisioning section, click the Authentication setting.
4. Toggle on Require two-factor authentication (2FA) for members. Once you enable this setting, you can click Download CSV to download a list of all members and their 2FA status.
5. Click Save.

Once you enable the 2FA requirement:

- Members that are not enrolled in 2FA have their sessions revoked and will be required to set up 2FA on their next login
- An email is sent to workspace and organization admins notifying them of the 2FA requirement

Enforced 2FA for guests

Who is impacted:

- Applies to all supported login methods
- Affected guests must enable 2FA to regain access.

Enforced 2FA restricts access to all Figma content across web, desktop, and mobile platforms. Open sessions remain unaffected until the guest logs out or their session expires.

Your organization's admins can configure this feature through the administration portal in your Figma account. It is a self-service feature.

1. Go to the Admin console.
2. Click the Settings tab.
3. Select Guest Membership and locate the toggle for 2FA for Guests.
4. Review the number of guests who will be blocked, then click Save.

Once activated, Org admins will receive an email notification and affected guests will receive an email prompting them to enable 2FA to regain access to files within their organization. Affected users are blocked from content access right away, so we recommend activating 2FA for Guests during non-peak hours.

Invite new guests to an organization where 2FA for guests is enabled

- Guests with 2FA enabled: Receive and accept invitations as usual.
- Guests without 2FA: Can accept invitations but won't access files until they enable 2FA on their account.

By enforcing 2FA for guests, organizations can safeguard sensitive data while maintaining a seamless collaboration experience for properly authenticated users.

Multiple identity provider (IdP) support

Admins can connect more than one identity provider (IdP) to their organization. This allows you to:

- Support multiple authentication methods across different business units or regions
- Run parallel IdPs during migration or consolidation projects
- Offer flexibility for hybrid IT environments

How it works

- Admins can configure multiple IdPs directly in their admin settings.
- Domain-based routing: Figma routes users to the correct IdP based on their email domain. Each domain maps to exactly one IdP at a time, and a single IdP can serve multiple domains.

Set up multiple IdPs

1. From the file browser, select Admin in the sidebar.
2. Click the Settings tab.
3. In the Login and provisioning section, click select Manage identity providers (IdP).
4. Click + Add IDP to add a new provider.
5. In the modal, select Edit configuration to update the identify provider and SAML Single Sign On (SSO) configuration details.
    1. Choose your provider type.

2. Provide IdP details (such as metadata URL, entity ID, or signing certificate). For more information on setting up identify providers, see Guide to SAML SSO.
3. Select one or more domains whose members should authenticate with this IdP.
4. Test sign-in using an email on a mapped domain to confirm it's working correctly.
5. Repeat for additional IdPs as needed.

The Identity providers table will show each IdP and its mapped domains.

- Select an identify provider from the table to edit IdP details or domain mappings.
- To remove an IdP, hover over an IdP on the table and select More > Remove. Be sure to remap domains first (either all to one IdP or to different IdPs) to prevent login disruption.
- Users on unmapped domains won't be able to sign in with SSO.
    - Figma Enterprise: If your organization allows any login method, those users can still sign in with other methods.
    - Figma for Government: Invited users can sign in with a magic link.

Set internal policies for your organization

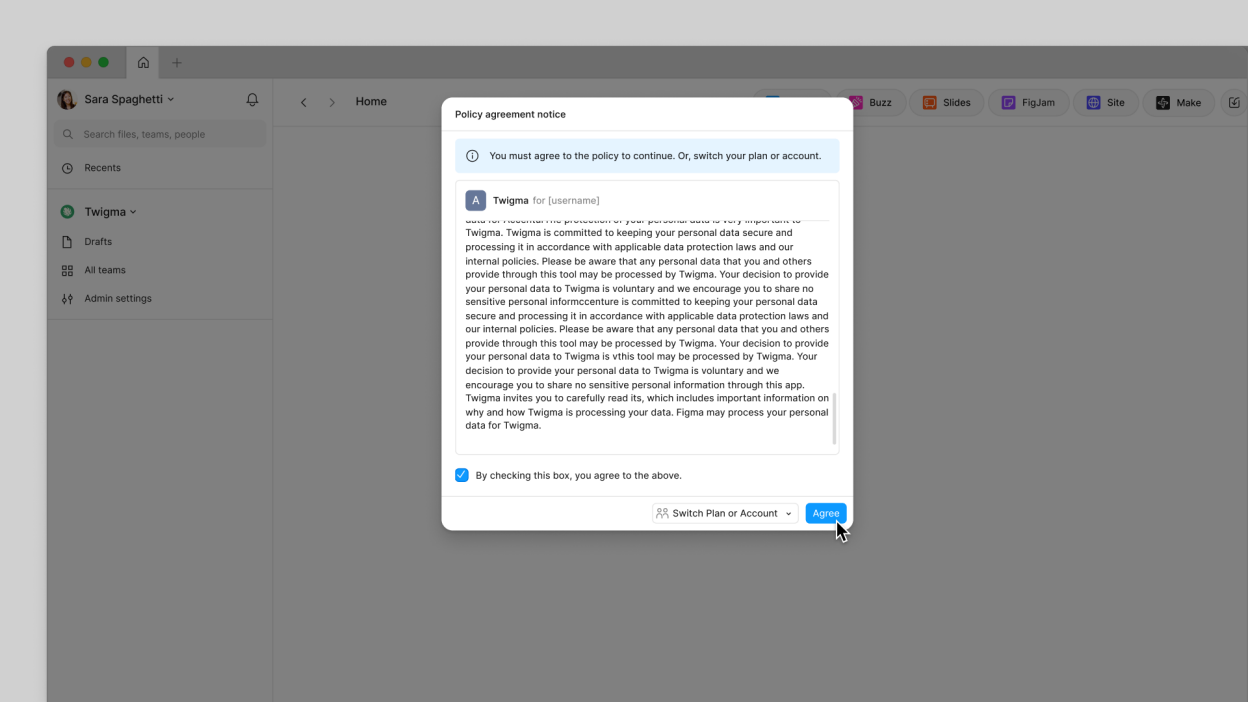
Internal policies let you require people in your organization to review and agree to custom policies before accessing content. For example, you can require members to review and agree to your company's internal privacy policy before continuing to work in Figma.

To enable internal policies for your organization, contact Figma's support team.

When you contact support, include the following details:

- Audience: Who must agree to the policy (members, guests, or everyone)
- Cadence: How often users must agree to the internal policy (once per year, or once per user lifetime)

When an internal policy is enabled, users in the selected audience will be blocked by a modal containing the policy the next time they navigate to any content or page in the organization. Users must agree to the policy before they can continue. If the policy cadence is set to once per year, users will be required to agree to the policy again each year.



Review if internal policies are enabled or disabled

Admins can review if an internal policy is set for an organization.

1. From the file browser, click Admin
2. Select the Settings tab.
3. In the Other section, review if Internal policies are enabled or disabled

Note: To change this setting and or to update the content of your internal policy, you'll need to reach out to Figma's Support team. Whenever a policy is enabled or disabled, organization admins will receive an email that includes the policy's enabled or disabled date, cadence, audience, policy title, and the full policy text.

Enterprise Key Management (EKM)

Enterprise Key Management (EKM) allows eligible organizations to encrypt certain Figma file data at rest using the organization's own AWS Key Management Service (KMS) key. This provides additional control over data at rest—you can grant, monitor, and revoke Figma's access to the encryption key at any time.

To request EKM for your organization, contact the Figma team. After you share the required details, our team will coordinate the setup on Figma's side.

What data is encrypted with EKM?

EKM applies to file data stored in Figma's backend that's stored in AWS S3, including:

- File checkpoints (shapes, text, frames, layers, etc.)
- Images and videos uploaded to files

The following data is not encrypted using EKM:

- Metadata
- Comments
- Component definitions stored in databases

For a full list of data that stored locally, see Enabled localized file hosting.

Request EKM setup

To set up EKM, contact Figma. You'll receive instructions to create AWS KMS keys and grant access to Figma's AWS account. After you provide the details below, Figma's team will configure EKM for your organization and confirm when it's active.

Include the following in your request:

- Primary AWS KMS key ARN
- Replica AWS KMS key ARN (for disaster recovery replication)
- Confirmation that Figma's AWS account has been granted the required permissions for both keys

Note: Once enabled, EKM automatically applies to all new files in your organization. Existing files will be encrypted gradually in the background, and do not require any modifications to your workflows.

Monitor key usage

You can monitor key activity through AWS CloudTrail, which logs encryption, decryption, and key access events performed by Figma's IAM roles.

EKM and localized file hosting

Figma supports using EKM alongside data locality. If your organization uses data locality, we recommend configuring data locality first and then enabling EKM.

Important considerations

- AWS KMS only: Currently, only AWS KMS is supported.
- One key per organization: EKM uses one AWS KMS key for all encrypted file data in the organization. Different keys per workspace, project, or team aren't supported.

Caution: If Figma loses access to your AWS KMS key (for example, if permissions are revoked or the key is unavailable), all users in your organization will be logged out and Figma will be inaccessible until access is restored.
Note: At this time, Figma doesn't fully support offboarding from EKM. If EKM is disabled, existing files remain encrypted with your key and you'll need to maintain access to that key for future decryption.

Guest access expiration

Guest expiration helps organization admins control how long external collaborators can access their organization.

By default, guests don't expire and can remain in the organization indefinitely. With Governance+, admins can choose to add expiration dates for guests—either individually or by setting a plan-wide default that applies to new guests going forward.

How it works

Guest access expiration includes two related controls:

- Per-guest expiration: By default, guests have no expiration date. Admins can add, update, or remove an expiration date for guests at any time, individually or in bulk.
- Plan-wide default (optional): Organization admins can set a default number of days that applies to newly invited guests.
    - This setting only affects guests who join after the default is set.
    - A guest's expiration countdown begins when they join the organization.

Here are some additional details about guest expiration:

- When a guest reaches their expiration date, they're automatically removed from the organization and any paid seat they occupied returns to the available pool of seats for others to use.
- Expiration dates appear in the People tab of your admin, and all expiration-related changes are recorded in the activity log.

- Guests that are within two weeks of their expiration date see an in-product banner that indicates how much time remains before their access ends.

Set default duration for guest access

Organization admins can optionally set a default duration (in days) that applies to newly invited guests.

To set a default guest expiration:

1. From the file browser, click Admin.
2. Select the Settings tab.
3. Under External access, open Guest membership.
4. Find Set default duration for guest access, enter a number of days, and click Save.

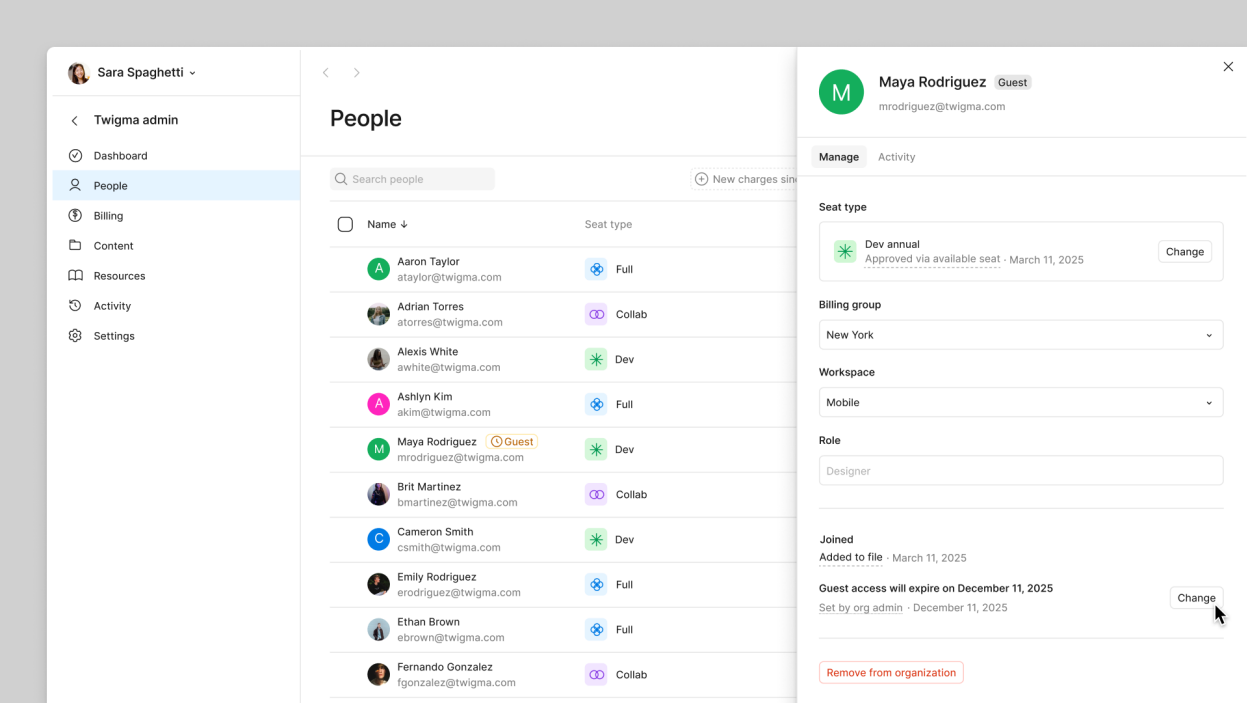
Change a guest's expiration date

Admins can manage expiration dates for guests directly from the admin dashboard. They can apply expiration dates individually or in bulk.

Organization admins

To change a guest's expiration date:

1. From the file browser, click Admin and select the People tab.
2. Locate and select the guest to open the side panel with member details.
3. Under Guest access expiration date, click Change. Enter a date and click Save. To make a guest permanent, select Remove expiration date instead. You can re-add an expiration date at any time.



To bulk apply or remove expiration dates:

1. From the file browser, click Admin and select the People tab.
2. Select the checkboxes next to the guests you want to update.
3. In the bulk action bar, select Set guest expiration date.
4. Enter a date and click Save. To make a guest permanent, select Remove expiration date instead. You can re-add an expiration date at any time.

Workspace admins

Workspace admins can manage guest expiration for users in workspaces they manage.

1. From the file browser, click Admin in the left sidebar.
2. Select the relevant workspace in the sidebar.
3. Select the Members tab.
4. Locate and select the guest to open the side panel with member details.
5. Under Guest access expiration date, click Change. Enter a date and click Save. To make a guest permanent, select Remove expiration date instead. You can re-add an expiration date at any time.

To bulk apply or remove expiration dates:

1. From the file browser, click Admin in the left sidebar.
2. Select the relevant workspace in the sidebar.
3. Select the Members tab.

4. Select the checkboxes next to the guests you want to update.
5. In the bulk action bar, select Set guest expiration date.
6. Enter a date and click Save. To make a guest permanent, select Remove expiration date instead. You can re-add an expiration date at any time.

AI hosting controls

FedRAMP limits access to particular models in Bedrock, so this feature is not available in Figma for Government.
AI hosting controls lets Governance+ organization admins choose how AI traffic is routed.

When enabled:

- For all features governed by the AI toggle, when the feature needs to leverage an AI model, we route the request to a multi-tenant Amazon Web Services account that Figma owns
- We then process the request on Amazon Web Services (AWS) uusing models hosted in Figma's AWS environment, including Amazon Bedrock and Amazon SageMaker. AI data won't be sent to non-AWS providers. This means AI data won't be sent to APIs outside of Figma’s AWS environment e.g. OpenAI, Anthropic, or Google Cloud Platform etc.

Enable AI hosting controls

Organization admins can restrict AI traffic for an entire organization:

1. From the admin, go to settings.
2. Under in the AI section, click on AI controls.
3. In the AI features modal, if AI is enabled anywhere in the organization (i.e. at the plan-level and/or for any workspace), you can choose to restrict AI traffic by toggling on Restrict AI traffic to Figma’s AWS environment. This control governs all traffic in the plan, regardless of where it originated. If AI is disabled everywhere, you cannot restrict AI traffic.

Be aware that when traffic is restricted, output quality may vary and some AI features will not be available. The list of unavailable AI features may change over time:

1. Remove Object
2. Separate Layers
3. Boost Resolution

4. Edit Image
5. Expand Image
6. Vectorize

Developer Logs API

The Developer Logs API lets you fetch a granular log of API calls made to the REST API or MCP server within your organization. This is a companion to the more low-volume, high-signal security and compliance logs available through Activity Logs.

For setup and implementation, refer to the Developer Logs API documentation:

- Figma Enterprise: developers.figma.com
- Figma for Government: developers.figma-gov.com

Product-Specific Terms

Last Updated: March 11, 2026

If you use the offerings and settings described below, the applicable Product-Specific Terms apply and are expressly incorporated into your existing customer agreement with Figma (your "**Customer Agreement**"). Capitalized terms used and not defined in the Product-Specific Terms have the meanings given to them in the Customer Agreement. These terms will govern if they conflict with any of the other terms in your Customer Agreement.

1. **Beta Features and Free Trials**.

a. Product features clearly identified as Alpha or Beta features as well as any features, products, or services provided on a free trial or promotional basis (collectively "**Early Access Features**") made available by Figma are provided to Customer for testing and evaluation purposes only. Figma does not make any commitment to provide Alpha or Beta features in any future versions of the Figma Platform. Figma may immediately and without notice remove Alpha or Beta features for any reason without liability to Customer. Any features, products, or services provided on a free trial basis will be free of charge until the earlier of (a) the end of the evaluation period set forth by Figma in writing (email sufficient), or (b) the start date of any purchased subscriptions ordered by Customer for the feature, product, or service being evaluated under the trial, or (c) termination by Figma in its sole discretion. Customer is not obligated to use Early Access Features.

b. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, ALL EARLY ACCESS FEATURES ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, WITHOUT ANY PERFORMANCE OBLIGATIONS, AND FIGMA SHALL HAVE NO INDEMNIFICATION OBLIGATIONS NOR LIABILITY OF ANY TYPE WITH RESPECT TO THE EARLY ACCESS FEATURES UNLESS SUCH EXCLUSION OF LIABILITY IS NOT ENFORCEABLE UNDER APPLICABLE LAW IN WHICH CASE FIGMA'S LIABILITY WITH RESPECT TO THE EARLY ACCESS FEATURES SHALL NOT EXCEED $1,000.00.

c. ANY DATA CUSTOMER ENTERS INTO THE FIGMA PLATFORM DURING A FREE TRIAL MAY BE PERMANENTLY LOST UNLESS CUSTOMER PURCHASES A SUBSCRIPTION TO THE FIGMA PLATFORM TRIALED, AN UPGRADE TO THE SUBSCRIPTION TRIALED, OR EXPORTS SUCH DATA, BEFORE THE END OF THE TRIAL PERIOD.

d. To the extent Customer provides Figma feedback concerning any Early Access Features, Customer hereby grants Figma the right to use such feedback to maintain, improve, and enhance Figma's products and services.

2. **AI Features**. The Figma AI Terms attached hereto and available at figma.com/legal/ai-terms outline additional terms and conditions that apply to use of Figma artificial intelligence features, including the AI-related settings that apply to Customer Content, and the pricing and payment terms for AI credits.

3. **[Reserved]**

4. **Community & APIs**. The Figma Developer Terms attached hereto and available at www.figma.com/developer-terms/ apply to use of Figma's Application Programming Interfaces, Software Development Kits, and related documentation. The Figma Community Terms attached hereto and available at figma.com/legal/community-terms/ apply to use of Figma Community.

5. **Desktop and Mobile Apps**. Figma's desktop and mobile applications ("**Figma Apps**") are licensed (not sold) to end users. Subject to the terms and conditions of this Agreement, Figma hereby grants Customer a license within the Territory, on a limited, non-exclusive, revocable, non-transferable, and non-sublicensable basis for Authorized Users to install the Figma Apps on a device that is owned or controlled by an Authorized User and to use the Figma Apps in support of its authorized use of the Figma Platform during the Order Term under this Agreement. If Customer fails to comply with any of the terms or conditions of this Agreement, in accordance with the Disputes Clause (Contract Disputes Act), Customer must immediately cease using the Figma Apps and uninstall and delete the Figma Apps from all Authorized User devices.

6. **Apple-Specific Terms for Figma Apps**. In addition to Customer's agreement with the terms and conditions of this Agreement, and notwithstanding anything to the contrary in this Agreement, the following provisions apply with respect to your use of any version of the Figma Apps compatible with the iOS operating system of Apple Inc. ("**Apple**"). Apple is not a party to this Agreement and does not own and is not responsible for the Figma Apps. Apple is not providing any warranty for the Figma Apps except, if applicable, to refund the purchase price for it. Apple is not responsible for maintenance or other support services for the Figma Apps and shall not be responsible for any other claims, losses, liabilities, damages, costs or expenses with respect to the Figma Apps, including any third-party product liability claims, claims that any Figma App fails to conform to any applicable legal or regulatory requirement, claims arising under consumer protection or similar legislation, and claims with respect to intellectual property infringement. Any inquiries or complaints relating to the use of the Figma Apps, including those pertaining to intellectual property rights, must be directed to Figma in accordance with the Notices section herein. The license Customer has been granted herein is limited to a non-transferable license to use the Figma Apps on an Apple-branded product that runs Apple's iOS operating system and is owned or controlled by an Authorized User, or as otherwise permitted by the Usage Rules set forth in Apple's App Store Terms of Service, except that the Figma Apps may also be accessed and used by other accounts associated with the Authorized User via Apple's Family Sharing or volume purchasing programs. In addition, Customer's use of the Figma Apps is governed by the terms of any third-party agreement applicable to Customer when using the Figma Apps, such as Customer's wireless data service agreement. Figma's right to

enter into, rescind or terminate any variation, waiver or settlement under this Agreement is not subject to the consent of any third party.

Figma AI Terms

1. Access to Figma AI. Figma AI is made available to Customer on the terms and conditions that apply to the Figma Platform in the Customer Agreement. Just like when Customer uses the Figma Platform generally, Customer is responsible for using Figma AI in accordance with Figma's Acceptable Use Policy. "Figma AI" means feature(s) and functionality made available by Figma within the Figma Platform that are identified by Figma as artificial intelligence (AI) features.

2. Input, Output, and Ownership. Customer may provide or make available prompts, images, materials, files, and other content to Figma AI ("Input"), and receive images, materials, files, and other content (such as code) generated and returned by Figma AI based on that Input ("Output"). Input and Output are Customer Content. As between Customer and Figma, Customer retains all right, title, and interest in Customer's Input and Output, and Figma retains all right, title, and interest in the Figma Platform (including improvements and enhancements to the Figma Platform, along with new products and features). "Customer Content" means the applications and materials that Customer develops on or uploads to the Figma Platform.

3. [Reserved]

4. [Reserved]

5. AI Limitations. Output is generated by artificial intelligence. Output is not verified by Figma for accuracy and does not represent Figma's views. Figma makes no warranty or guarantee as to the accuracy, completeness, or reliability of Output and will in no way be liable or responsible for Customer's use of Output or any omissions or errors in Output. Customer is responsible for evaluating Output for accuracy and suitability for Customer's use case, including by employing human review of Output and obtaining any relevant clearances.

6. Figma AI Credits.

Every seat comes with a set number of Credits, depending on Customer's Figma subscription and seat type, as described in the Documentation.

With notice at least 30 days prior to a future renewal, Figma may switch models to offer an AI Credits Subscription - an annual subscription detailed in the Documentation that aligns with Customer's existing Figma subscription term. The AI Credits Subscription will be billed and payable annually upfront. The same billing, payment, renewal, and cancellation terms as Customer's underlying Figma subscription apply. Customer's AI Credits Subscription added

or upgraded during the subscription term will be charged from the date of purchase and prorated to the end of the subscription term.

6.1. Credit Details. Credits (i) do not represent legal tender, currency, or stored value; (ii) are not redeemable for monetary value; (iii) are not exchangeable or transferable; (iv) can only be used for Figma AI features on the Figma Platform; and (v) expire at the end of the set period and do not rollover. If Customer is eligible for a refund or credit for an AI Credits Subscription, that refund or credit is solely based on the time remaining in the subscription term, and not on the number of unused Credits. Promotional Credits provided by Figma free of charge are considered an Early Access Feature. To learn more about how Credits work, visit this Help Center article.

7. Miscellaneous. Figma may non-materially update these Figma AI Terms in the same manner that Figma may update the Customer Agreement. Figma AI made available in beta is also governed by the beta terms found in the Customer Agreement or, if there are no beta terms in the Customer Agreement, then in Figma's Terms of Service. Any capitalized terms that are used but not defined in these Figma AI Terms will have the meaning given to those terms in the Customer Agreement. If the term "Figma Platform" is not used in the Customer Agreement, Figma Platform has the same meaning as the term used to refer to Figma's products and services.

Community Terms

These Figma Community Terms (“Community Terms”) govern your access to, use of, and participation in Figma Community. Figma Community is a platform, available at figma.com/community, through which users of Figma’s products and services can access templates and other resources developed by other users.

If you are agreeing to these Community Terms on behalf of a company (such as your employer) or other legal entity, you represent and warrant that you have the authority to bind that company or other legal entity to these Community Terms. In that case, “you” refers to that company or other legal entity. These terms are expressly incorporated into your existing customer agreement with Figma (your “Customer Agreement”). Figma Community is made available to you on the terms and conditions that apply to the Figma Platform in your Customer Agreement, as supplemented by these Community Terms (notwithstanding anything to the contrary in your Customer Agreement). These terms will govern if they conflict with any of the other terms in your Customer Agreement.

Overview. Figma users can share and sell templates, plug-ins, widgets, and other resources (“Community Resources”) with other users on Figma Community. Any user who makes Community Resources available to the Figma Community is referred to as a "Community Creator." Figma is the Community Creator for those Community Resources that expressly identify Figma as the creator. All other Community Resources are developed and made available by third parties that are not affiliated with Figma. If you provide Community Resources to Figma users through the Figma Community as a Community Creator, you are also subject to the Creator Agreement.

License to Community Resources. If you use any third-party Community Resources available on Figma Community, you agree that (a) such Community Resources constitute “Non-Figma Resources” as defined in your Customer Agreement, (b) you are obtaining a license to the Community Resource directly from the Community Creator (not Figma) and therefore your license is subject to the terms entered into between you and the Community Creator, (c) Figma does not and will not have any responsibility or liability under any agreement between you and a Community Creator (or to enforce any such agreement); and (d) by obtaining any Community Resource on Figma Community, you authorize Figma to share your relevant data with the Community Creator (including your name and information reasonably related to the transaction), any other information

shared between you and the Community Creator (if any) is governed by the Community Creator’s privacy policy.

Community Purchases. If you purchase any third-party Community Resources on Figma Community, you acknowledge and agree that Figma is acting as the Community Creator’s disclosed commercial agent for the sale, so you are required to make any payments directly to Figma and you expressly authorize Figma or Figma’s third-party payment processor to charge you for such Community Resources. The applicable fees, including any recurring fees, for Community Resources are specified during the payment process.

Community Reviews and Comments. If you write any reviews or provide any public comments on Figma Community, you authorize Figma and its service providers to use that content to provide Figma Community and to maintain, improve, and enhance Figma’s products and services.

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 brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Figma 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.

Reserved.

Disclaimer & Limitation of Liability. FIGMA WARRANTS THAT THE FIGMA COMMUNITY AND COMMUNITY RESOURCES WILL PERFORM SUBSTANTIALLY IN ACCORDANCE WITH THE DOCUMENTATION. EXCEPT AS EXPRESSLY SET FORTH IN THE FOREGOING, NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THESE COMMUNITY TERMS OR YOUR CUSTOMER AGREEMENT, FIGMA COMMUNITY AND COMMUNITY RESOURCES (WHETHER PROVIDED BY FIGMA OR A THIRD PARTY) ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, WITHOUT ANY PERFORMANCE OBLIGATIONS, AND FIGMA SHALL HAVE NO INDEMNIFICATION OBLIGATIONS NOR LIABILITY OF ANY TYPE WITH RESPECT TO FIGMA COMMUNITY OR COMMUNITY RESOURCES UNLESS SUCH EXCLUSION OF LIABILITY IS NOT ENFORCEABLE UNDER APPLICABLE LAW IN WHICH CASE FIGMA’S LIABILITY WITH RESPECT TO FIGMA COMMUNITY OR COMMUNITY RESOURCES SHALL NOT EXCEEDTHE AMOUNT CUSTOMER PAID FOR THE SERVICE. For the avoidance of doubt, any service level agreements or commitments provided in your Customer Agreement do not apply to Community Resources (whether provided by Figma or a third party).

Miscellaneous. Figma may non-materially modify these terms at any time. Figma will post the most current version of these Terms on www.figma.com/product-specific-terms/. Figma will endeavor to provide you with reasonable advance notice of any change to the terms that, in our sole determination, materially affects your rights or your use of Figma Community. Figma may provide you this notice through Figma Community, on Figma's website, and/or by email to the email address associated with your account. By continuing to use Figma Community or any Community Resource after any non-materially revised terms become effective, you agree to be bound by the new non-materially modified terms. Any capitalized terms that are used but not defined in these terms will have the meaning given to those terms in your Customer Agreement. If the term "Figma Platform" is not used in your Customer Agreement, Figma Platform has the same meaning as the term used to refer to Figma's products and services.

Figma Developer Terms

These Figma Developer Terms (“Terms”) apply to any use of Figma, Inc.’s (“Figma”, “we” or “us”) Application Programming Interfaces, Software Development Kits, Model Context Protocol servers, and related resources and documentation (collectively, “Developer Resources”). The term “you” or “your” means the person using the Developer Resources. If you are an individual using the Developer Resources on behalf of a company (such as your employer) or other legal entity, then “you” or “your” means that entity and you represent and warrant that you have the authority to bind that entity to these Terms.

1. Other Applicable Terms. These Terms do not grant you any right to access or use our online collaboration tools (the “Services”), which are instead governed by a separate agreement with us (the “Agreement”). Your access to and use of Developer Resources are subject to these Terms and the Agreement. To the extent these Terms conflict with the Agreement, these Terms control. All Developer Resources must be used in accordance with Figma’s Acceptable Use Policy.

2. License. Subject to these Terms, we grant you a non-exclusive, royalty free, worldwide (except to the extent prohibited by applicable law), non-transferable (subject to the section titled “Assignment”, below), limited license to access and use the Developer Resources only as necessary to develop, test, and support an integration or other connection (collectively, a “Figma Integration”) with the Services as permitted in Figma’s associated developer documentation.

3. Security.

a. You will (i) not share any keys or credentials obtained for use of the Developer Resources (“Credentials”), (ii) keep Credentials and all login information secure and confidential, and (iii) use Credentials as your sole means of accessing the Developer Resources. You must use the Credential type designated by Figma for your Figma Integration's use case, as described in Figma's developer documentation.

b. If you develop a Figma Integration, you will ensure your Figma Integration adheres to industry-best security and privacy practices. You represent and warrant that your Figma Integration does not contain any security vulnerabilities and operates with the Developer Resources in a secure manner.

4. Limitations.

a. Figma may conduct security testing on Figma Integrations, including, at Figma's option and in Figma's sole discretion, penetration testing and submission to bug bounty programs. Figma may audit Figma Integrations for compliance with law and our terms or policies. You will use commercially reasonable efforts to cooperate with such audits.

b. Figma may update or change Developer Resources in Figma's sole discretion. Figma will use commercially reasonable efforts to ensure that changes to Developer Resources are backward compatible. If Figma deprecates any Developer Resources, Figma will use commercially reasonable efforts to notify you in advance. Changes to the Developer Resources may require you to download new or different copies of the Developer Resources, and you agree to update to the latest version of the Developer Resources promptly after any update.

c. Figma may suspend or terminate your and/or your Figma Integration's access to the Developer Resources if Figma believes (in good faith) that you have violated these Terms.

d. Reserved

e. Figma may have or develop products or features that may be competitive with Figma Integrations. Nothing in these Terms are intended to impair Figma's right to develop, make, use, procure, or market such products or features now or in the future or to require Figma to compensate you in any way related to Figma Integrations.

f. To provide the most value to Figma and Figma users that use the Developer Resources, Figma Integrations must allow data to flow both directions. Figma may disallow any Figma Integrations from using Figma APIs if they block write-back tool calls.

5. WARRANTY & LIABILITY DISCLAIMER. FIGMA WARRANTS THAT ALL DEVELOPER RESOURCES WILL PERFORM SUBSTANTIALLY IN ACCORDANCE WITH THE DOCUMENTATION. EXCEPT AS EXPRESSLY SET FORTH IN THE FOREGOING, ALL DEVELOPER RESOURCES ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, WITHOUT ANY PERFORMANCE OBLIGATIONS, AND FIGMA SHALL HAVE NO INDEMNIFICATION OBLIGATIONS NOR LIABILITY OF ANY TYPE WITH RESPECT TO THE DEVELOPER RESOURCES UNLESS SUCH EXCLUSION OF LIABILITY IS NOT ENFORCEABLE UNDER APPLICABLE LAW IN WHICH CASE FIGMA'S LIABILITY WITH RESPECT TO THE DEVELOPER

RESOURCES SHALL NOT EXCEEDTHE AMOUNT CUSTOMER PAID FOR THE SERVICE.

6.Reserved.

7. Publicly Available Integrations. If your Figma Integration is made available to users outside your organization, then the following additional restrictions and requirements apply:

a. Once the Figma Integration is available, you may not materially change the purpose or nature of the Figma Integration. You may always choose to create a new Figma Integration or take down an existing Figma Integration.

b. If your Figma Integration processes Integration Data, you must: (i) obtain from users all necessary rights, permissions, and consents for your access, collection, storage, sharing and other processing of any Integration Data; (ii) provide and maintain a clear and conspicuous privacy policy which notifies users that you (and not Figma) are responsible for the privacy, security, and integrity of any Integration Data you process; and (iii) process such data solely in accordance with applicable laws, your terms with your users, and your privacy policy. “Integration Data” means content and data collected through or used by a Figma Integration, including information about end users or others with whom they interact through the Services, or any information relating to an identifiable natural person or otherwise governed by privacy laws.

c. You and your Figma Integration will employ technical, administrative, and physical safeguards that: (i) comply with applicable laws and regulations, including privacy laws; and (ii) protect the confidentiality, integrity, and availability of Integration Data, including Integration Data that relates to any identifiable natural person and other information governed by privacy laws.

d. You must notify us immediately upon becoming aware of a Security Incident. You will preserve evidence regarding the Security Incident, and provide us with information we request regarding the Security Incident. You agree to take such actions, at your expense, as Figma may reasonably request to respond to, investigate, and mitigate adverse effects of any Security Incident. Before you communicate with the public (e.g., via press release, blogs, or social media) or any third party about a Security Incident, you will consult with Figma regarding such communication, to the extent doing so does not unreasonably interfere with your investigation or remediation of the Security Incident or your compliance with your legal obligations. “Security Incident” means the accidental, unlawful, or unauthorized access to, use, disclosure, alteration, loss, or

destruction of (i) the Developer Resources; (ii) Integration Data; and/or (iii) your Figma Integration.

8. General Terms.

a. Ownership. As between the parties, Figma owns all right, title, and interest in the Developer Resources, the Services, and any data derived from either, and you own all right, title, and interest in your Figma Integrations (excluding any Developer Resources). Except as explicitly stated in these Terms, each party retains all right, title, and interest in and to its intellectual property rights. All rights not expressly granted are reserved, and no license or other right should be implied under these Terms.

b. Feedback. To the extent that you give Figma feedback, comments, or suggestions concerning the Developer Resources or Services (collectively, “Feedback”), you hereby grant Figma the right to use such Feedback to maintain, improve, and enhance Figma’s products and services.

c. Publicity. We may use your name (“Marks”) for marketing or promotional purposes, including listing your Figma Integration in our directories to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71. Any goodwill that accrues to your Marks from our use in accordance with this Section will inure exclusively to you.

d. Early Access Features. Developer Resources clearly identified as Alpha or Beta features (collectively “Early Access Features”) made available by Figma are provided to you for testing purposes only, and Figma does not make any commitment to provide Early Access Features. You are not obligated to use Early Access Features. Figma may immediately and without notice remove Early Access Features for any reason without liability to you. Notwithstanding anything to the contrary in these Terms, all Early Access Features are provided "as is" without warranty of any kind and without any performance obligations.

e. Reserved.

f. Export Restrictions. You represent and warrant that you are not located in, under the control of, or a national or resident of any country on the United States Commerce Department’s Table of Denial Orders. In connection with these Developer Terms, you will comply with all applicable import, re-import, sanctions, anti-boycott, export, and re-export control laws and regulations, including all such laws and regulations that apply to a U.S. company.